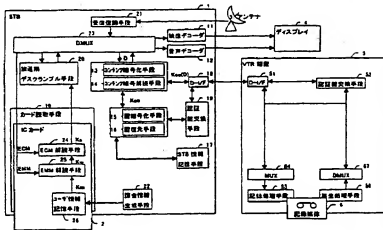




(51) 国際特許分類 <b>G11B 20/10, H04N 5/91</b>	<b>A1</b>	(11) 国際公開番号 <b>WO99/38164</b>  (43) 国際公開日 1999年7月29日(29.07.99)
(21) 国際出願番号 <b>PCT/JP99/00292</b>  (22) 国際出願日 1999年1月25日(25.01.99)  (30) 優先権データ 特願平10/12474 1998年1月26日(26.01.98) 特願平10/27572 1998年2月9日(09.02.98)  (71) 出願人 (米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)(JP/JP) 〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP) (72) 発明者: および (75) 発明者/出願人 (米国についてのみ) 山田正純(YAMADA, Masazumi)(JP/JP) 〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP) 飯塚裕之(IITSUKA, Hiroyuki)(JP/JP) 〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP) 後藤昌一(GOTO, Shoichi)(JP/JP) 〒576-0021 大阪府交野市妙見坂5-4-204 Osaka, (JP) 武知秀明(TAKECHI, Hidetaki)(JP/JP) 〒533-0004 大阪府大阪市東淀川区小松4丁目11-10 201号 Osaka, (JP)	(74) 代理人 弁理士 松田正道(MATSUDA, Masamichi) 〒532-0003 大阪府大阪市淀川区宮原5丁目1番3号 新大阪生島ビル Osaka, (JP)  (81) 指定国 CN, KR, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)  添付公開書類 国際調査報告書	
(54) Title: <b>METHOD AND SYSTEM FOR DATA RECORDING / REPRODUCING, APPARATUS FOR RECORDING/REPRODUCING, AND MEDIA FOR RECORDING PROGRAM</b>  (54) 発明の名称 データ記録再生方法、データ記録再生システム、記録装置、再生装置、プログラム記録媒体  (57) Abstract Digital data subjected to first encryption with a content key are recorded together with the content key subjected to second encryption. When the encrypted digital data and the encrypted content key are reproduced, the encrypted content key is decrypted and the decrypted content key is used to recover the digital data.		



- |                               |   |
|-------------------------------|---|
| 3 ... IC CARD                 | 17 ... STB INFORMATION STORAGE MEANS      |
| 4 ... ANTENNA                 | 18 ... VERIFICATION KEY EXCHANGE MEANS    |
| 5 ... DISPLAY                 | 19 ... BROADCAST SCRAMBLER MEANS          |
| 6 ... VTR UNIT                | 20 ... RECEIVER-DEMODULATION MEANS        |
| 7 ... RECORDING MEDIUM        | 21 ... ORANGE INFORMATION GENERATOR MEANS |
| 8 ... CARD READER MEANS       | 22 ... STB DECODER MEANS                  |
| 9 ... VIDEO RECODER MEANS     | 23 ... SMP DECODER MEANS                  |
| 10 ... AUDIO RECODER MEANS    | 24 ... USER INFORMATION STORAGE MEANS     |
| 11 ... CONTENTS ENCODER MEANS | 25 ... VERIFICATION KEY EXCHANGE MEANS    |
| 12 ... CONTENTS DECODER MEANS | 26 ... RECORDING PROCESSING MEANS         |
| 13 ... KEY ENCODER MEANS      | 27 ... REPRODUCTION PROCESSING MEANS      |
| 14 ... KEY DECODER MEANS      |   |

ディジタルデータにコンテンツ鍵を用いて第1の暗号化を施した暗号化ディジタルデータと、前記コンテンツ鍵に第2の暗号化を施した暗号化コンテンツ鍵とを記録媒体に記録し、記録された前記暗号化ディジタルデータおよび前記暗号化コンテンツ鍵を再生し、前記暗号化コンテンツ鍵を解読して得られた前記コンテンツ鍵を用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得ることを特徴とするデータ記録再生方法。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦	ES スペイン	LI リヒテンシュタイン	SG シンガポール
AL アルバニア	FR フランス	LK スリ・ランカ	SI スロヴェニア
AM アルメニア	GB ガボン	LR リベリア	SK スロバキア
AT オーストリア	GD グレナダ	LS リトアニア	SL シェラ・レオネ
AU オーストラリア	GE ジョージア	LT リトアニア	SN セネガル
AZ アゼルバイジャン	GG ガーナ	LU ルクセンブルグ	SZ スワジランド
BA ボスニア・ヘルツェゴビナ	GM ガンビア	LV ラトヴィア	TD チャド
BB バルバドス	GN ギニア	MC モナコ	TG トーゴ
BBE ベルギー	GW ギニア・ビサウ	MD モルドヴァ	TJ タジキスタン
BBF ブルガリア	GR ギリシャ	MG マダガスカル	TL トルコ
BBG ベナン	HR クロアチア	MK マケドニア	TM トルクメニスタン
BBR ブラジル	HU ハンガリー	ML モリタニア	TR トリニダード・トバゴ
BBY ベラルーシ	ID インドネシア	MR モリタニア	UA ウクライナ
CA カナダ	IE アイルランド	MW マラウイ	UG ウガンダ
CF 中央アフリカ	IL イスラエル	MX メキシコ	US 米国
CG コンゴ	IN インド	NE ニジェール	UZ ウズベキスタン
CH スイス	IS アイスランド	NL オランダ	VN ヴェトナム
CI コートジボアール	IT イタリア	NZ ノールウェー	YU ユーゴスラビア
CM カメルーン	JP 日本	NO ノルウェー	ZA 南アフリカ共和国
CN 中国	KE ケニア	PT ポルトガル	ZW ジンバブエ
CU キューバ	KG キルギスタン	RO ルーマニア	
CY キプロス	KR 韓国	RU ロシア	
CZ チェコ	KZ カザフスタン	SD スーダン	
DE ドイツ	LC セントルシア	SE スウェーデン	
DK デンマーク			
EE エストニア			

## 明 細 書

データ記録再生方法、データ記録再生システム、記録装置、再生装置、プログラム記録媒体

## 技術分野

本発明は、著作権等により再生についての期間や回数が制限された、デジタルデータを記録するデータ記録装置と、そのデジタルデータを再生するデータ再生装置、データ記録再生システムおよびデータ記録再生方法に関するものである。

## 背景技術

現在、著作権保護の対象となっている映画や音楽等のAVデータは、ビデオテープ等に格納されている。ユーザは、そのようなビデオテープ等を有料で貸し出すレンタル店を通じて、例えば1週間というような所定の期間のみビデオテープ等を借り、それを再生することによって、映画や音楽等を鑑賞することができる。

他方、上述したビデオテープ等のレンタルのシステムとは別に、デジタル技術や暗号化技術の進歩等から、放送局からの映画や音楽等の番組を通信衛星を介して入力し、その番組をコンテンツ暗号化してビデオテープ等に記録し、再生する装置が考えられる。

衛星放送の録画、再生をユーザーが自由に行えると、少数のユーザーを介して、不特定多数の者に、録画された番組が無制限に供給されることが可能

になるため、この対策を講ずることは、プロバイダにとって必要不可欠なことである。まず、希望の番組を視聴する場合の手順について説明する。ユーザーが視聴希望の番組を選択すると、その番組の視聴料金に対応する視聴用課金情報が、ICカードに記録される。原則として各番組のデータには、スクランブルがかけられており、当該番組の視聴用課金情報が、ICカードに記録されている場合のみ、STBがスクランブルを解除して、スクランブルがない状態でディスプレイが映像出力する。ただし、STBがスクランブルを解除しても、当該AVデータにはコピー防止信号（マクロビジョン）がかかっているため、この状態で、記録媒体に記録しても、再生時の再生画像が乱れてしまう。

次に、希望の番組を録画／再生する場合の手順について説明する。ユーザーが録画希望の番組を選択すると、その番組の録画料金に対応する録画用課金情報が、ICカードに記録される。当該番組の録画用課金情報が、ICカードに記録されている場合のみ、STBが前述したマクロビジョンを解除して、乱れないAVデータをVTR装置に出力し、VTR装置は、これを記録媒体に記録する。記録されたAVデータは、マクロビジョンがかかってないため、通常のAVデータと同様の再生方法で、映像出力が得られる。

以上の手順で、ICカードに記録された視聴用課金情報および録画用課金情報は、一定期間分が電話回線等によって、プロバイダに通知される。STB装置とVTR装置が分離したタイプの衛星放送のデータ記録再生システムについて説明したが、各装置の機能を一つの装置に集約したタイプのももある。

ところで、上述したビデオテープ等のレンタルのシステムは、これからの

多チャンネルデジタル放送時代においても、ユーザがその都度レンタル店に出向いてビデオテープ等を借りなければならないという点など、ユーザにとって相変わらず手間がかかり不便である。

しかしながら、上述した記録再生方法では、一度記録された記録媒体は、何回でも再生でき、また、当該記録媒体を複製することも容易に行えるという問題点がある。

従来の記録再生装置では、映画や音楽等の著作権保護の対象となっているＡＶデータの有効再生期間や有効再生回数には制限がないことになる。例えば、劇場放映直後の映画のように、特別な価値を有するＡＶデータが上述したような、再生の期間や回数について制限のない記録再生装置によって記録媒体に記録されると、そのＡＶデータの価値は半減する。つまり、放送局は、そのような特別な価値を有するＡＶデータを安心して放送することができない。

上記問題点の対策として、ＡＶデータが記録された記録媒体に、当該ＡＶデータ記録時に使用したＳＴＢおよび／またはＶＴＲ装置のＩＤも記録しておき、ＩＤが異なる機器で再生しようとする、再生できないようにするという方法が提案されている。しかし、ＩＤ識別機能を有しない機器を用いる場合は、ＩＤの一致に関わりなく再生が可能であるという課題がある。また、全ての機器がＩＤ識別機能を有するとの前提に立てば、機器固有のＩＤを用いているために、当該機器が修復不可能な故障・破損等によって、使用できなくなった場合には、当該記録媒体に記録されたＡＶデータは、再生が不可能になってしまうという課題がある。

## 発明の開示

本発明は、上述した従来のデータ記録再生方法の課題を考慮し、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供することを第一の目的とするものである。

また、前記第一の目的に加え、記録および／または再生時に、確実に課金可能なデータ記録再生方法およびデータ記録再生システムを提供することを目的とするものである。

さらに、前記第一の目的に加え、再生時のロスタイムが少ないデータ記録再生システムを提供することを目的とするものである。

また、本発明は、データを記録媒体に記録し、そのデータの有効再生期間や有効再生回数の制限を遵守する記録装置および再生装置を提供することを目的とするものである。

## 図面の簡単な説明

図 1 は、本発明の第 1 の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図 2 は、本発明の第 1 の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図 3 は、本発明の第 1 の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図 4 は、本発明の第 1 の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。

図5は、本発明の第2の実施の形態におけるデータ記録再生システムで記録された記録媒体の貸与時の流れを示すフロー図である。

図6は、本発明の第3の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図7は、本発明の第3の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図8は、本発明の第4の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図9は、本発明の第4の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図10は、本発明の第5の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図11は、本発明の第5の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図12は、本発明の第5の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図13は、本発明の第5の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

図14は、本発明の第5の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図15は、本発明の第6の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図16は、本発明の第6の実施の形態におけるデータ記録再生システムの

データ記録時のデータの流れを示すフロー図である。

図17は、本発明の第6の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図18は、本発明の第6の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

図19は、本発明の第6の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図20は、本発明の第6の実施の形態における別のデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図21は、本発明の第7の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図22は、本発明の第7の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図23は、本発明の第8の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

図24は、本発明の第8の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

図25は、本発明の第8の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

図26は、本発明の第9の実施の形態の記録装置および再生装置のブロック図である。

図27は、本発明の第9の実施の形態の記録装置および再生装置に使用される鍵暗号化鍵Kxリストの一例を示す図である。



図 28 は、図 26 とは異なる本発明の記録装置および再生装置のブロック図である。

図 29 は、図 26 または 28 とは異なる本発明の記録装置および再生装置のブロック図である。

図 30 は、図 26、28 または 29 とは異なる本発明の記録装置および再生装置のブロック図である。

図 31 は、図 26、28、29 または 30 とは異なる本発明の記録装置および再生装置のブロック図である。

#### 発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

##### (第 1 の実施の形態)

以下に、本発明の第 1 の実施の形態を図面を参照して説明する。

図 1 は、本発明の第 1 の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムは、本発明のチューナ装置に対応する STB (Set Top Box ; 衛星放送受信機) 1 と、STB 1 にユーザー ID 等の情報を与える IC カード 2 と、STB 1 に接続されているアンテナ 3 およびディスプレイ 4 と、本発明の VTR 装置に対応する VTR 装置 5 と、VTR 装置 5 によってデータを記録／再生される記録媒体 6 とから構成されている。

STB 1 は、IC カード 2 に記録された情報の読み取り、必要情報を IC カード 2 に記録するカード読取手段 10 と、STB 1 の機器 ID 等の情報を

記憶するSTB情報記憶手段17と、ディスプレイ4に対してデコードされたAVデータを出力する映像デコーダ11および音声デコーダ12と、コンテンツ鍵を生成し、AVデータに前記コンテンツ鍵を用いて暗号化を施して暗号化AVデータを生成するコンテンツ暗号化手段13と、前記コンテンツ鍵に第2の暗号化を施して暗号化コンテンツ鍵を生成する鍵暗号化手段15と、前記暗号化コンテンツ鍵を解読して前記コンテンツ鍵を復元する鍵暗号解読手段16と、復元された前記コンテンツ鍵を用いて前記暗号化AVデータを解読して、前記AVデータを得るコンテンツ暗号解読手段14と、VTR装置5と直接データの伝達を行うD-I/F（デジタルインターフェイス）18およびVTR装置5と認証鍵の交換を行ってVTR装置5の確認を行う認証鍵交換手段19と、人工衛星からの電波をアンテナ3を介して受信して、受信したデータの復調を行いSTB1内部用の信号に変換する受信復調手段21と、受信したデータに施されている放送用暗号を解除する放送用デスクランブル手段20と、多重化されている受信データを分離するDMUX（Demultiplexer；分離部）23とを有している。なお、STB1は、上記の他に、STB1の装置全体を制御するSTB制御手段（図示せず）を備えている。

VTR装置5は、STB1と直接データの伝達を行うD-I/F（デジタルインターフェイス）51およびSTB1と認証鍵の交換を行ってSTB1の確認を行う認証鍵交換手段52と、前記暗号化AVデータおよび前記暗号化コンテンツ鍵に対して記録媒体6のフォーマットに適合した多重化を行うMUX（Multiplexer；多重化部）54および多重化されたデータを記録媒体6に記録する記録処理手段55と、記録媒体6に記録された

データを再生する再生処理手段 58 および多重化された再生データを分離する DMUX (De-multiplexer ; 分離部) 57 とを備えている。なお、VTR 装置 5 は、上記の他に、VTR 装置 5 の装置全体を制御する VTR 制御手段 (図示せず) を備えている。

次に、このような本実施の形態の動作を説明する。

まず、AV データを記録媒体 6 に記録する時のデータの流れを図 2 を用いて説明する。図 2 は、本発明の第 1 の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図 2 において、図 1 で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、D は、記録しようとする AV データの生 (Plain) データを、Kco は、AV データ D の暗号化に用いるコンテンツ鍵を、Kco (D) は、AV データ D にコンテンツ鍵 Kco を用いて暗号化を施して得られる暗号化 AV データを、STBPa は、コンテンツ鍵 Kco の暗号化に用いる STB 1 に固有の公開鍵を、STBPa (Kco) は、コンテンツ鍵 Kco に公開鍵 STBPa を用いて暗号化を施して得られる暗号化コンテンツ鍵を、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、コンテンツ鍵 Kco を、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

先ず、受信復調手段 21 は、アンテナ 3 を介して受信した、放送局からの、デジタルの映像データ、音声データ、EMM (個別情報)、ECM (番組情報) および暗号化された放送スクランブル鍵 Ks を入力し、映像データおよび音声データの信号波形の乱れを整形し、映像データ、音声データ、E

MM、ECMおよび暗号化された放送スクランブル鍵 $K_s$ をDMUX 23に出力する。

EMM（個別情報）は、後に説明するワーク鍵 $K_w$ という鍵を生成するさいに必要な情報である。

さらに、ECM（番組情報）は、暗号化された放送スクランブル鍵 $K_s$ を復元するさいに必要な情報である。

その後、DMUX 23は、受信復調手段21からの映像データ、音声データ、EMM、ECMおよび放送スクランブル鍵 $K_s$ を入力して分離し、映像データおよび音声データ（AVデータ）を放送デスクランブル手段20に出力する。また、EMMをEMM解読手段25に出力し、ECMおよび暗号化された放送スクランブル鍵 $K_s$ をECM解読手段24に出力する。

次に、EMM解読手段25は、ユーザID鍵 $K_m$ を入力するとともに、DMUX 23からのEMMを入力し、ユーザID鍵 $K_m$ でEMMを解読してワーク鍵 $K_w$ を生成し、ECM解読手段24に出力する。

さらに、ECM解読手段24は、EMM解読手段25からのワーク鍵 $K_w$ を入力するとともに、DMUX 23からの、ECMおよび暗号化された放送スクランブル鍵 $K_s$ を入力し、ワーク鍵 $K_w$ でECMを解読して、暗号化された放送スクランブル鍵 $K_s$ の暗号化を復元し、放送デスクランブル手段20に出力する。

そして、放送デスクランブル手段20は、ECM解読手段24からの放送スクランブル鍵 $K_s$ を入力するとともに、DMUX 23からの、スクランブルされたAVデータを入力し、放送スクランブル鍵 $K_s$ で、スクランブルされたAVデータをデスクランブルする。

AVデータDは、放送用のスクランブルを放送用デスクランブル手段20で解除され、DMUX23で分離されて、生のAVデータDとなって、映像デコーダ11および音声デコーダ12およびコンテンツ暗号化手段13へ送られる。映像デコーダ11および音声デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、ディスプレイ4へ出力する。

コンテンツ暗号化手段13は、コンテンツ鍵Kcoを生成し、生成したコンテンツ鍵Kcoを用いて、AVデータDに暗号化を施して、暗号化AVデータKco(D)を生成する。生成されたコンテンツ鍵Kcoは、鍵暗号化手段15へ送られ、鍵暗号化手段15は、STB情報記憶手段17に記憶されているSTB1に固有の公開鍵STBPaを用いて、コンテンツ鍵Kcoに暗号化を施して、暗号化コンテンツ鍵STBPa(Kco)を生成する。

暗号化AVデータKco(D)は、D-I/F18を介して、暗号化コンテンツ鍵STBPa(Kco)は、認証鍵交換手段19およびD-I/F18を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換手段19、52は、D-I/F18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

VTR装置5へ伝達された暗号化AVデータKco(D)は、D-I/F51を介して、暗号化コンテンツ鍵STBPa(Kco)は、D-I/F51および認証鍵交換部52を介して、それぞれMUX54へ送られて、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理手段55によって、記録媒体6に記録される。

次に、記録媒体6に記録されたAVデータを再生する時のデータの流れを図3を用いて説明する。図3は、本発明の第1の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図3において、図1で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。STBSaは、公開鍵STBP aに対応し、暗号化コンテンツ鍵STBP a (Kco) を解読してコンテンツ鍵Kcoを復元するのに用いるSTB1に固有の秘密鍵を示す。図中の他の記号は、図2に倣う。

多重化されて記録媒体6に記録された暗号化AVデータKco (D) および暗号化コンテンツ鍵STBP a (Kco) は、再生処理手段58により再生され、DMUX 57で分離される。

分離された暗号化AVデータKco (D) は、D-I/F 51を介して、分離された暗号化コンテンツ鍵STBP a (Kco) は、認証鍵交換手段52およびD-I/F 51を介して、それぞれSTB1へ伝達されるが、それに先だって、記録時と同様に、STB1、VTR装置5それぞれの認証鍵交換手段19、52は、D-I/F 18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

STB1へ伝達された暗号化AVデータKco (D) は、D-I/F 18を介して、コンテンツ暗号解読手段14へ送られ、暗号化コンテンツ鍵STBP a (Kco) は、D-I/F 18および認証鍵交換手段19を介して、鍵暗号解読手段16へ送られる。鍵暗号解読手段16は、STB情報記憶手段17に記憶されているSTB1に固有の秘密鍵STBSaを用いて、暗号化コンテンツ鍵STBP a (Kco) をコンテンツ鍵Kcoに復元して、コンテンツ暗号解読手段14へ送る。コンテンツ暗号解読手段14は、復元されたコン

テンツ鍵Kcoを用いて、暗号化AVデータKco(D)を解読して得られるAVデータDを、映像デコーダ11および音声デコーダ12へ出力する。映像デコーダ11および音声デコーダ12は、AVデータDに施された高エネルギー符号化処理等をデコードし、ディスプレイ4へ出力する。

以上の手順にしたがって、AVデータを記録/再生することにより、AVデータに暗号化を施すのに用いたコンテンツ鍵にSTB1に固有の公開鍵を用いて暗号化を施して、暗号化されたAVデータと一緒に記録媒体に記録し、再生時には暗号化されたコンテンツ鍵をSTB1に固有の秘密鍵を用いて復元しているため、STB1に固有の秘密鍵を持っているシステム、すなわち、STB1そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

次に、本実施の形態におけるデータ記録再生システムの課金方法について説明する。本課金方法は、AVデータの記録/再生時に課金するものであるため、図2、図3を参照して説明する。

まず、記録時の課金方法について説明する。図2において、STB1のSTB制御手段(図示せず)は、記録時に、課金情報生成手段22を用いて課金情報を生成し、これをカード読取手段10を介して、ICカード2に記録させる。記録のタイミングとしては、例えば、ユーザーからの記録指令に連動して記録するとしてもよいし、コンテンツ暗号化手段13または鍵暗号化手段15の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容としては、課金の金額そのものを記録するものであってもよいし、課

金内容を特定するための識別子のようなものであってもよい。

次に、再生時の課金方法について説明する。図3において、STB1のSTB制御手段(図示せず)は、再生時に、課金情報生成手段22を用いて課金情報を生成し、これをカード読取手段10を介して、ICカード2に記録する。記録のタイミングとしては、例えば、ユーザーからの再生指令に連動して記録するとしてもよいし、コンテンツ暗号解読手段14または鍵暗号解読手段16の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容については、記録時と同様である。

ICカード2に記録された課金情報は、定期的または不定期に、衛星放送のサービスプロバイダに対して、電話回線等の通信を介して出力され、サービスプロバイダは、この課金情報に基づいて、ユーザーの銀行口座からの引き落とし等の方法によって、ユーザーから課金の徴収を行う。

なお、上記説明において、課金情報は記録時および再生時に記録する、すなわち、記録、再生の両方に対して課金を行うとして説明したが、これに限らず、いずれか一方についてのみ、課金を行うとしてもよい。

また、課金情報は、カード読取手段10を介して、ICカード2に記録されるときとして説明したが、これに限らず、例えば、STB情報記憶手段17に記録されるとしてもよい。なお、STB情報記憶手段17に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ICカード2およびカード読取手段10を省いてもよい。

また、再生時の課金情報は、再生期間の限定および/または再生回数の限定を伴っていてもよい。例えば、ある期間を過ぎる、またはある再生回数を超えると、課金の金額が変わるというものでもよい。ただし、再生回数の限



定を伴う場合には、再生する毎に、記録媒体 6 等に通算再生回数を示す情報を書き込む必要がある。

さらに、記録時に、再生時の課金情報を生成するために必要な情報を、記録媒体 6 に記録し、記録媒体 6 の再生時に前記必要な情報を用いて課金情報を生成するとしてもよい。このときは、例えば、STB 制御手段が記録時に前記必要な情報を生成し、これを、D-I/F 18 および 51 を介して、記録処理手段 55 に送り、記録処理手段 55 は、記録データの最初にこれを記録する。再生時には、前記必要な情報は、再生処理手段 58 によって再生され、D-I/F 18 および 51 を介して、STB 制御手段へ送られ、STB 制御手段は、これに基づいて、課金情報生成手段 22 を用いて再生時の課金情報を生成する。

以上説明したところから、本実施の形態におけるデータ記録再生システムは、記録および/または再生時に、確実に課金が可能なデータ記録再生システムであることがわかる。

次に、本実施の形態におけるデータ記録再生システムによって、記録媒体に記録されるデータの、記録媒体上の記録領域について、図 2、図 4 を参照して説明する。

図 4 は、本発明の第 1 の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。図 4 の左右方向は、記録媒体 6 の時間的な記録位置を示し、上下方向は、同時刻に記録されたデータの構成を示す。図 4 において、記録領域は、メインエリアとサブエリアとに分けられており、メインエリアには、暗号化 AV データと、コンテンツ鍵変更のタイミングを示すフラグとが書き込まれており、サブエリア

には、当該記録位置に対応するメインエリアの位置に記録された暗号化AVデータ (Kco-a (D)、Kco-b (D)、Kco-c (D)、Kco-d (D)、...) の暗号化に用いられたコンテンツ鍵 (Kco-a、Kco-b、Kco-c、Kco-d、...) に、公開鍵 STBPa を用いて暗号化を施して得られた、暗号化コンテンツ鍵 (STBPa (Kco-a)、STBPa (Kco-b)、STBPa (Kco-c)、STBPa (Kco-d)、...) と、次のコンテンツ鍵の切替後に用いられるコンテンツ鍵 (Kco-b、Kco-c、Kco-d、Kco-e、...) に、公開鍵 STBPa を用いて暗号化を施して得られた、暗号化コンテンツ鍵 (STBPa (Kco-b)、STBPa (Kco-c)、STBPa (Kco-d)、STBPa (Kco-e)、...) とが書き込まれている。ただし、図4中においては、暗号化コンテンツ鍵 STBPa (Kco-a)、STBPa (Kco-b)、STBPa (Kco-c)、STBPa (Kco-d)、... は、便宜上、暗号化前のコンテンツ鍵 Kco-a、Kco-b、Kco-c、Kco-d、... で表現している。

前述したように、コンテンツ暗号化手段13は、コンテンツ鍵Kcoを定期的または不定期的に切り替えて生成し、生成したコンテンツ鍵Kcoを用いて、AVデータDに暗号化を施して、暗号化AVデータKco (D) を生成するが、現在使用中のコンテンツ鍵 (例えば、Kco-a) の次の切替後のコンテンツ鍵 (例えば、Kco-b) をあらかじめ生成して、その使用に先立って、鍵暗号化手段15により暗号化コンテンツ鍵STBPa (Kco-a) に変換して、認証鍵交換手段19、D-I/F18、51を介して、MUX54へ送り、記録処理手段55は、これを現在使用中のコンテンツ鍵Kc

o-a、それによって暗号化された暗号化AVデータKc o-a (D)等とともに、図4に示した記録領域に記録する。なお、コンテンツ鍵変更のタイミングを示すフラッグは、例えば、AVデータを伝送するパケットヘッダに付加されて伝達されてくるものとし、記録処理手段55は、これをもとに、各記録データの記録位置を決定する。

図4に示すように、切り替えの後のコンテンツ鍵、例えば、Kc o-b、に対応する暗号化コンテンツ鍵 STB P a (Kc o-b)は、切り替えの前のコンテンツ鍵Kc o-aに対応する暗号化AVデータKc o-a (D)の少なくとも一部と重なるように、記録媒体6に記録されており、切り替えの前のコンテンツ鍵Kc o-aは、それに対応する暗号化AVデータKc o-a (D)が記録されている位置に重なって、記録媒体6に記録されている。なお、暗号化コンテンツ鍵 STB P a (Kc o-b)の記録領域は、図4においては、その次のコンテンツ鍵Kc o-cに対応する暗号化コンテンツ鍵 STB P a (Kc o-c)が書き込まれる直前まで書き込まれているが、少なくとも暗号化コンテンツ鍵 STB P a (Kc o-c)が書き込まれる前に書き込みが終了していればよい、すなわち、図4中の暗号化コンテンツ鍵 STB P a (Kc o-b)の記録領域は、少なくとも暗号化AVデータKc o-a (D)の一部と重なるように記録されておれば、暗号化コンテンツ鍵 STB P a (Kc o-c)の記録領域の始端との間にデータの空白領域があってもよい。

以上の記録要領によって、記録媒体への記録を行うことによって、再生時には、次のコンテンツ鍵をあらかじめ解読できるので、本実施の形態におけるデータ記録再生システムは、再生時のロスタイムが少ないデータ記録再生システムであることがわかる。

なお、本発明の記録媒体上の記録領域への記録要領は、本実施の形態における上述した記録要領に限るものではなく、例えば、コンテンツ暗号化手段13が次の切替後のコンテンツ鍵をあらかじめ生成せず、VTR装置5が、STB1から送られてくるデータを一時記憶する手段を有し、前記一時記憶する手段に現在のデータを一時記憶させて、コンテンツ鍵切替後のデータを受け取った後に、記録媒体6への記録領域を決定して、記録するとしてもよい。

また、上述した記録要領に加えて、コンテンツ鍵Kc oの暗号化に用いた鍵を特定できる情報を記録媒体6に記録するとしてもよい。具体的には、本実施の形態においては、STB1のID情報である。この情報を利用して、例えば、STB1以外のSTBを用いて再生をしようとした場合、当該STBでは再生できない旨の警告とともに、再生可能なSTB（ここではSTB1）のID情報を表示することができる。

また、暗号化コンテンツ鍵を記録媒体6中の外部に出力されないデータ領域に記録してもよい。例えば、D-VHSシステムであれば、サブコード領域に記録する。これによって、さらに、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムとなる。

さらに、本実施の形態においては、暗号化デジタルデータおよび暗号化コンテンツ鍵は、記録媒体上の再生のタイミングに対応する記録位置に記録されるとして説明したが、これに限るものではなく、記録位置にとらわれず、切り替えの後のコンテンツ鍵に対応する暗号化コンテンツ鍵が、切り替えの前のコンテンツ鍵に対応する暗号化デジタルデータの少なくとも一部とタイミング的に重なるように、また、一つのコンテンツ鍵に対応する暗号化

コンテンツ鍵が、それに対応する暗号化デジタルデータとタイミング的に重なるように、再生されさえすればよい。

なお、上述した本実施の形態の課金方法および／または記録媒体上の記録領域への記録要領の替わりに、従来のものをを用いる場合においては、上述したそれぞれの効果は得られないものの、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供するという、本発明の第一の目的は満足するものである。

#### (第2の実施の形態)

以下に、本発明の第2の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明のチューナ装置の機器モデルに対して固有な鍵である点に関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第1の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

本実施の形態においては、コンテンツ鍵Kc oの暗号化にSTB 1の機器モデルに固有の公開鍵STBUP aを用い、コンテンツ鍵Kc oを復元するのにSTB 1の機器モデルに固有の秘密鍵STBUS aを用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。したがって、本実施の形態の動作は、図2、図3において、公開鍵 STB P a、秘密鍵 STB

S a および暗号化コンテンツ鍵 STB P a ( K c o ) を、それぞれ、公開鍵 STB U P a、秘密鍵 STB U S a および暗号化コンテンツ鍵 STB U P a ( K c o ) に置き換えたもので示されるので、詳細の説明は、図 2、図 3 に倣うとして省略する。

以上の手順にしたがって、AV データを記録／再生することにより、本実施の形態は、第 1 の実施の形態によって得られる効果に加え、図 5 に示すように、STB 1 と同じモデルである STB 1 0 1 を所有しているユーザー間での記録媒体 6 の貸し借りが可能となり、かつ、STB 1 が修復不可能な故障・破損等によって、使用できなくなった場合においても、同じ機器モデルの STB に代替すれば、引き続き使用できるものであることがわかる。

### (第 3 の実施の形態)

以下に、本発明の第 3 の実施の形態を図面を参照して説明する。本実施の形態が上述した第 1 の実施の形態と異なる点は、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明の IC カードに記録されたユーザ ID に対して固有な鍵である点に関する点である。したがって、本実施の形態において、第 1 の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第 1 の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第 1 の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

図 6 は、本発明の第 2 の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図 7 は、本発明の第 2 の

実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図6、図7に示すとおり、本実施の形態においては、コンテンツ鍵Kc oの暗号化にICカード2に記録されたユーザIDに対して固有の公開鍵USERPaを用い、コンテンツ鍵Kc oを復元するのにユーザIDに対して固有の秘密鍵USERSaを用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。

以上の手順にしたがって、AVデータを記録／再生することにより、本実施の形態は、第1の実施の形態によって得られる効果に加え、STB1が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のSTB（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、ICカード2と一緒に記録媒体6の貸し借りをすれば、他のユーザーの使用が可能となるものであることがわかる。

また、本実施の形態において、上述のようにコンテンツ鍵Kc oの暗号化にICカード2に記録されたユーザIDに対して固有の公開鍵USERPaを用いて、暗号化コンテンツ鍵USERPa（Kc o）を生成するとともに、同じくICカード2に記録された他のユーザIDに対して固有の公開鍵 USER1Paを用いて、暗号化コンテンツ鍵 USER1Pa（Kc o）も生成して、暗号化コンテンツ鍵USERPa（Kc o）とともに、記録媒体6に記録しておけば、ICカード2を貸し出さなくても、公開鍵 USER1Paに対応する秘密鍵 USER1Saを保持している特定のユーザーは、その USER1Saを用いて暗号化コンテンツ鍵 USER1Pa（Kc o）を復元できるので、その特定のユーザーに対してのみ、記録媒体6の貸し出し使用が可能となる。なお、公開鍵 USER1Paは、単数に限るものではなく、公開鍵 USER1Pa～USERnPaと、複数個

であってもよい。すなわち、ユーザーは、貸し出し使用をしたい他のユーザーが生じた場合には、所定の手続を経て、ICカード2に、当該他のユーザーに対応する公開鍵  $USERnPa$  を記録して貰うことによって、当該他のユーザーへの簡単な貸し出し使用が可能となるものである。

なお、上記動作からわかるように、本実施の形態においては、図1に示した第1の実施の形態におけるデータ記録再生システムの構成から、STB記憶手段11を省略したものであってもよい。

#### (第4の実施の形態)

以下に、本発明の第4の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明のICカードに記録されたサービスに対して固有な鍵である点に関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第1の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

図8は、本発明の第4の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図9は、本発明の第4の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図8、図9に示すとおり、本実施の形態においては、コンテンツ鍵  $Kco$  の暗号化にICカード2に記録されたサービスに対し



て固有の公開鍵SERV P aを用い、コンテンツ鍵K c oを復元するのにS T B 1の機器モデルに固有の秘密鍵SERV S aを用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。ここで、サービスに対して固有の鍵とは、具体的には、特定の番組に対してのみ固有、特定のジャンルの番組に対してのみ固有、特定のチャンネル番組に対してのみ固有、特定の衛星放送のプロバイダに対してのみ固有の鍵等が挙げられる。

例えば、特定の番組の記録／再生に対して、前もって料金を支払うことにより、その番組に固有の公開鍵SERV P aおよび秘密鍵SERV S aをI Cカード2に記憶させてもらうことにより、前記特定の番組の記録／再生が可能となるものである。この場合、公開鍵SERV P aおよび秘密鍵SERV S aがI Cカード2に記憶されていなければ、記録できなくなる措置をS T B 1が有する必要がある。なお、公開鍵SERV P aおよび秘密鍵SERV S aが必要な特定の番組以外の番組に対しては、第1～第3の実施の形態のいずれかで用いた公開鍵および秘密鍵に切り替えて、これらを用いるという、併用も可能である。

以上の手順にしたがって、A Vデータを記録／再生することにより、本実施の形態は、第1の実施の形態によって得られる効果に加え、S T B 1が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のS T B（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、記録されたA Vデータに対応する特定のサービスを享受することを許可された特定のユーザーに対してのみ、記録媒体6の貸し借り使用が可能となるものであることがわかる。

なお、上記動作からわかるように、本実施の形態においては、図1に示した第1の実施の形態におけるデータ記録再生システムの構成から、S T B記

憶手段 11 を省略したものであってもよい。

(第 5 の実施の形態)

以下に、本発明の第 5 の実施の形態を図面を参照して説明する。本実施の形態が上述した第 1 の実施の形態と異なる点は、本発明の鍵暗号化手段が VTR 装置に備えられており、それに伴って、本発明のチューナ装置が、コンテンツ鍵を共通鍵によって暗号化する第二の鍵暗号化手段を有し、本発明の VTR 装置が、前記共通鍵によって暗号化された前記コンテンツ鍵を解読する第二の鍵暗号解読手段を有することに關する点である。したがって、本実施の形態において、第 1 の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第 1 の実施の形態と同じとする。

図 10 は、本発明の第 5 の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第 1 の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段 62 が、STB 1 ではなく、VTR 装置 5 に備えられており、それに伴い、STB 1 は、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段 31 を有し、VTR 装置 5 は、本発明の第二の鍵暗号解読手段に対応する鍵暗号解読手段 61 と、鍵暗号解読手段 61 および鍵暗号化手段 62 が用いる共通鍵、公開鍵等の情報を記憶する VTR 情報記憶手段 71 とを有している。また、STB 情報記憶手段 7 は、第 1 の実施の形態において保持していた情報に加えて、鍵暗号化手段 31 がコンテンツ鍵を暗号化するのに用いる共通鍵の情報を保持している。なお、第 1 の実施の形態と同様に、課金情報が、例えば、STB 情報記憶

手段 17 に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、IC カード 2 およびカード読取手段 10 を省いてもよい。

次に、このような本実施の形態の動作を説明する。

まず、AV データを記録媒体 6 に記録する時のデータの流れを図 11 を用いて説明する。図 11 は、本発明の第 5 の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図 11 において、図 10 で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図 2、図 3 に倣う。Kk は、コンテンツ鍵 Kco の暗号化に用いる STB 1 および VTR 装置 5 に共通な共通鍵を、AV データ D の暗号化に用いるコンテンツ鍵を、Kk (Kco) は、コンテンツ鍵 Kco に共通鍵 Kk を用いて暗号化を施して得られる暗号化コンテンツ鍵を、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、第 1 の実施の形態と同様に、コンテンツ鍵 Kco を、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

放送用電波として暗号化され、多重化された AV データ D は、アンテナ 3 を介して受信され、受信復調手段 21 で復調され、放送用の暗号を放送用デスクランブル手段 20 で解除され、DMUX 23 で分離されて、生の AV データ D となって、映像デコーダ 11 および音声デコーダ 12 およびコンテンツ暗号化手段 13 へ送られる。映像デコーダ 11 および音声デコーダ 12 は、AV データ D に施された高能率符号化処理等をデコードし、ディスプレイ 4 へ出力する。コンテンツ暗号化手段 13 は、コンテンツ鍵 Kco を生成し

、生成したコンテンツ鍵  $K_{co}$  を用いて、AVデータ  $D$  に暗号化を施して、暗号化AVデータ  $K_{co}(D)$  を生成する。生成されたコンテンツ鍵  $K_{co}$  は、鍵暗号化手段31へ送られ、鍵暗号化手段31は、STB情報記憶手段17に記憶されているSTB1およびVTR装置5に共通な共通鍵  $K_k$  を用いて、コンテンツ鍵  $K_{co}$  に暗号化を施して、暗号化コンテンツ鍵  $K_k(K_{co})$  を生成する。

暗号化AVデータ  $K_{co}(D)$  は、 $D-I/F18$  を介して、暗号化コンテンツ鍵  $K_k(K_{co})$  は、認証鍵交換手段19および $D-I/F18$  を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換手段19、52は、 $D-I/F18$  および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

VTR装置5へ伝達された暗号化AVデータ  $K_{co}(D)$  は、 $D-I/F51$  を介して、MUX54へ送られる。また、VTR装置5へ伝達された暗号化コンテンツ鍵  $K_k(K_{co})$  は、 $D-I/F51$  および認証鍵交換手段52を介して、鍵暗号解読手段61に送られる。鍵暗号解読手段61は、VTR情報記憶手段71に記憶されている共通鍵  $K_k$  を用いて、暗号化コンテンツ鍵  $K_k(K_{co})$  をコンテンツ鍵  $K_{co}$  に復元して、鍵暗号化手段62に送る。鍵暗号化手段62は、VTR情報記憶手段71に記憶されているSTB1に固有の公開鍵  $STBp_a$  を用いて、コンテンツ鍵  $K_{co}$  に暗号化を施して、暗号化コンテンツ鍵  $STBp_a(K_{co})$  を生成して、これをMUX54へ送る。MUX54へ送られた暗号化AVデータ  $K_{co}(D)$  および暗号化コンテンツ鍵  $STBp_a(K_{co})$  は、記録媒体6のフォーマットに適合し

た多重化を行われた後、記録処理手段 5 5 によって、記録媒体 6 に記録される。

次に、記録媒体 6 に記録された A V データを再生する時のデータの流れを図 1 2 を用いて説明する。図 1 2 は、本発明の第 5 の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図 1 2 からわかるように、本実施の形態においては、記録された暗号化コンテンツ鍵 STB P a ( K c o ) は、V T R 装置 5 内では復元されずに、S T B 1 の鍵暗号解読手段 1 6 へ送られ、ここで、S T B 情報記憶手段 1 7 に記憶されている S T B 1 に固有の秘密鍵 STB S a を用いることによって、コンテンツ鍵 K c o に復元される。図 1 で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。すなわち、A V データを再生する時のデータの流れは、第 1 の実施の形態の図 3 と同じになる。

以上の手順にしたがって、A V データを記録／再生することにより、A V データの記録時において、V T R 装置 5 への送信側である S T B 1 におけるコンテンツ鍵の暗号化が、負担の軽い共通鍵による暗号化としているので、A V データの暗号化およびコンテンツ鍵の暗号化を並行しておこなうことにより負担が増大している S T B 1 の負担を軽減できるので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第 1 の実施の形態におけるデータ記録再生システムと比較して、S T B 1 および V T R 装置 5 の負担を平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。

なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、第 1 の

実施の形態と同じく、本発明のチューナ装置（STB1）に対して固有な鍵であるとして説明したが、これに限るものではなく、例えば、第2～第4いずれかの実施の形態と同じく、本発明のチューナ装置（STB1）の機器モデルに対して固有な鍵、本発明のICカードに記録されたユーザIDに対して固有な鍵、本発明のICカードに記録されたサービスに対して固有な鍵であつてもよい。

また、本発明の公開鍵の情報は、本実施の形態においては、VTR情報記憶手段71に記憶されているものとして説明したが、これに限るものではなく、例えば、記録を始める際に、STB1から送られてくるとしてもよい。

なお、本実施の形態におけるデータ記録再生システムから、図13に示すように、鍵暗号化手段31および鍵暗号解読手段61を省略した構成も可能である。こうすれば、本発明のチューナ装置からVTR装置へのデータ送信において、コンテンツ鍵に暗号化を施さずに送信を行うことになる。このような構成は、後述する第8の実施の形態のように、STBおよびVTR装置の機能を一体化した一体化STBを備えるデータ記録再生システムに適用すると、特に有効である。以下に、図13の構成のデータ記録再生システムについて説明する。

図13の構成のデータ記録再生システムにおける、AVデータを記録媒体6に記録する時のデータの流れは、図14に示すようになる。図14において、図13で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図11、図12に倣う。

放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調手段21で復調され、放送用の暗号を放送用デ

スクランブル手段20で解除され、DMUX23で分離されて、生の(Plain)AVデータDとなって、映像デコーダ11および音声デコーダ12およびコンテンツ暗号化手段13へ送られる。映像デコーダ11および音声デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、ディスプレイ4へ出力する。コンテンツ暗号化手段13は、コンテンツ鍵Kcoを生成し、生成したコンテンツ鍵Kcoを用いて、AVデータDに暗号化を施して、暗号化AVデータKco(D)を生成する。

暗号化AVデータKco(D)は、D-I/F18を介して、コンテンツ鍵Kcoは、認証鍵交換手段19およびD-I/F18を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換手段19、52は、D-I/F18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

VTR装置5へ伝達された暗号化AVデータKco(D)は、D-I/F51を介して、MUX54へ送られる。また、VTR装置5へ伝達されたコンテンツ鍵Kcoは、D-I/F51および認証鍵交換手段52を介して、鍵暗号化手段62に送られる。鍵暗号化手段62は、VTR情報記憶手段71に記憶されているSTB1に固有の公開鍵STBP aを用いて、コンテンツ鍵Kcoに暗号化を施して、暗号化コンテンツ鍵STBP a(Kco)を生成して、これをMUX54へ送る。MUX54へ送られた暗号化AVデータKco(D)および暗号化コンテンツ鍵STBP a(Kco)は、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理手段55によって、記録媒体6に記録される。

図 13 の構成のデータ記録再生システムにおける、データ再生時のデータの流れについては、図 12 で示したデータ再生時のデータの流れと同じである。したがって、以下の説明を省略する。

なお、STB 情報記憶手段 17 および VTR 情報記憶手段 71 は、図 10 の構成において保持していた共通鍵の情報を保持している必要はない。

以上の手順にしたがって、AV データを記録／再生することにより、AV データの記録時において、VTR 装置 5 への送信側である STB 1 がコンテンツ鍵の暗号化を行わないので、AV データの暗号化およびコンテンツ鍵の暗号化を並行しておこなうことにより負担が増大している STB 1 の負担をさらに軽減できるので、図 13 の構成のデータ記録再生システムは、図 10 の構成のデータ記録再生システムと比較して、STB 1 および VTR 装置 5 の負担をさらに平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図 10 の構成のデータ記録再生システムと比較して、STB 1 から VTR 装置 5 へのデータ送信についてのセキュリティは低下する。このような構成は、後述する第 8 の実施の形態のように、STB および VTR 装置の機能を一体化した一体化 STB を備えるデータ記録再生システムに適用すると、特に有効である。

#### (第 6 の実施の形態)

以下に、本発明の第 6 の実施の形態を図面を参照して説明する。本実施の形態が上述した第 1 の実施の形態と異なる点は、本発明の鍵暗号化手段および鍵暗号解読手段が VTR 装置に備えられており、コンテンツ鍵の暗号化／復元を行う公開鍵／秘密鍵が、本発明の VTR 装置に対して固有な鍵であることに關する点である。したがって、本実施の形態において、第 1 の実施の



形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第 1 の実施の形態と同じとする。

図 15 は、本発明の第 6 の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第 1 の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段 6 2 および本発明の鍵暗号解読手段に対応する鍵暗号解読手段 6 4 が、STB 1 ではなく、VTR 装置 5 に備えられており、それに伴い、STB 1 は、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段 3 1 および本発明の第二の鍵暗号解読手段に対応する鍵暗号解読手段 3 2 を有し、VTR 装置 5 は、本発明の第二の鍵暗号解読手段に対応する鍵暗号解読手段 6 1 と、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段 6 3 と、鍵暗号解読手段 6 1、鍵暗号化手段 6 2、鍵暗号化手段 6 3 および鍵暗号解読手段 6 4 が用いる共通鍵、公開鍵等の情報を記憶する VTR 情報記憶手段 7 1 とを有している。また、STB 情報記憶手段 1 7 は、第 1 の実施の形態において保持していた情報に加えて、鍵暗号化手段 3 1 がコンテンツ鍵を暗号化するのに用いる共通鍵の情報を保持している。

なお、第 1 の実施の形態と同様に、課金情報が、例えば、STB 情報記憶手段 1 7 に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、IC カード 2 およびカード読取手段 1 0 を省いてもよい。

次に、このような本実施の形態の動作を説明する。

まず、AV データを記録媒体 6 に記録する時のデータの流れを図 1 4 を用いて説明する。図 1 6 は、本発明の第 6 の実施の形態におけるデータ記録再

生システムのデータ記録時のデータの流れを示すフロー図である。図16において、図15で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図2、図3に倣う。Kkは、コンテンツ鍵Kcoの暗号化に用いるSTB1およびVTR装置5に共通な共通鍵を、Kk(Kco)は、コンテンツ鍵Kcoに共通鍵Kkを用いて暗号化を施して得られる暗号化コンテンツ鍵を、VTRPaは、コンテンツ鍵Kcoの暗号化に用いるVTR装置5に固有の公開鍵を、VTRPa(Kco)は、コンテンツ鍵Kcoに公開鍵VTRPaを用いて暗号化を施して得られる暗号化コンテンツ鍵を、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、第1の実施の形態と同様に、コンテンツ鍵Kcoを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調手段21で復調され、放送用の暗号を放送用デスクランブル手段20で解除され、DMUX23で分離されて、生のAVデータDとなって、映像デコーダ11および音声デコーダ12およびコンテンツ暗号化手段13へ送られる。映像デコーダ11および音声デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、ディスプレイ4へ出力する。コンテンツ暗号化手段13は、コンテンツ鍵Kcoを生成し、生成したコンテンツ鍵Kcoを用いて、AVデータDに暗号化を施して、暗号化AVデータKco(D)を生成する。生成されたコンテンツ鍵Kcoは、鍵暗号化手段31へ送られ、鍵暗号化手段31は、STB情報記憶手段

17に記憶されているSTB1およびVTR装置5に共通な共通鍵Kkを用いて、コンテンツ鍵Kcoに暗号化を施して、暗号化コンテンツ鍵Kk(Kco)を生成する。

暗号化AVデータKco(D)は、D-I/F18を介して、暗号化コンテンツ鍵STBpa(Kco)は、認証鍵交換手段19およびD-I/F18を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換手段19、52は、D-I/F18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

VTR装置5へ伝達された暗号化AVデータKco(D)は、D-I/F51を介して、MUX54へ送られる。また、VTR装置5へ伝達された暗号化コンテンツ鍵Kk(Kco)は、D-I/F51および認証鍵交換手段52を介して、鍵暗号解読手段61に送られる。鍵暗号解読手段61は、VTR情報記憶手段71に記憶されている共通鍵Kkを用いて、暗号化コンテンツ鍵Kk(Kco)をコンテンツ鍵Kcoに復元して、鍵暗号化手段62に送る。鍵暗号化手段62は、VTR情報記憶手段71に記憶されているVTR装置5に固有の公開鍵VTRPaを用いて、コンテンツ鍵Kcoに暗号化を施して、暗号化コンテンツ鍵VTRPa(Kco)を生成して、これをMUX54へ送る。MUX54へ送られた暗号化AVデータKco(D)および暗号化コンテンツ鍵VTRPa(Kco)は、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理手段55によって、記録媒体6に記録される。

次に、記録媒体6に記録されたAVデータを再生する時のデータの流れを

図 17 を用いて説明する。図 17 は、本発明の第 6 の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図 17 において、図 15 で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。VTRS a は、公開鍵 VTRP a に対応し、暗号化コンテンツ鍵 VTRP a (Kco) を解読してコンテンツ鍵 Kco を復元するのに用いる VTR 装置 5 に固有の秘密鍵を示す。図中の他の記号は、図 16 に倣う。

多重化されて記録媒体 6 に記録された暗号化 AV データ Kco (D) および暗号化コンテンツ鍵 VTRP a (Kco) は、再生処理手段 58 により再生され、DMUX 57 で分離される。分離された暗号化コンテンツ鍵 VTRP a (Kco) は、鍵暗号解読手段 64 へ送られる。鍵暗号解読手段 64 は、VTR 情報記憶手段 71 に記憶されている VTR 装置 5 に固有の秘密鍵 VTRS a を用いて、暗号化コンテンツ鍵 VTRP a (Kw) をコンテンツ鍵 Kco に復元して、鍵暗号化手段 63 へ送る。鍵暗号化手段 63 は、VTR 情報記憶手段 71 に記憶されている共通鍵 Kk を用いて、コンテンツ鍵 Kco に暗号化を施して、暗号化コンテンツ鍵 Kk (Kco) を生成する。

分離された暗号化 AV データ Kco (D) は、D-I/F 51 を介して、生成された暗号化コンテンツ鍵 Kk (Kco) は、認証鍵交換手段 52 および D-I/F 51 を介して、それぞれ STB 1 へ伝達されるが、それに先だって、記録時と同様に、STB 1、VTR 装置 5 それぞれの認証鍵交換手段 19、52 は、D-I/F 18 および 51 を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

STB 1 へ伝達された暗号化 AV データ Kco (D) は、D-I/F 18 を介して、コンテンツ暗号解読手段 14 へ送られ、暗号化コンテンツ鍵 Kk

(Kco)は、D-I/F18および認証鍵交換手段19を介して、鍵暗号解読手段32へ送られる。鍵暗号解読手段32は、STB情報記憶手段17に記憶されている共通鍵Kkを用いて、暗号化コンテンツ鍵Kk(Kco)をコンテンツ鍵Kcoに復元して、コンテンツ暗号解読手段14へ送る。コンテンツ暗号解読手段14は、復元されたコンテンツ鍵Kcoを用いて、暗号化AVデータKco(D)を解読して得られるAVデータDを、映像デコーダ11および音声デコーダ12へ出力する。映像デコーダ11および音声デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、ディスプレイ4へ出力する。

以上の手順にしたがって、AVデータを記録/再生することにより、AVデータに暗号化を施すのに用いたコンテンツ鍵にVTR装置5に固有の公開鍵を用いて暗号化を施して、暗号化されたAVデータと一緒に記録媒体に記録し、再生時には暗号化されたコンテンツ鍵をVTR装置5に固有の秘密鍵を用いて復元しているため、VTR装置5に固有の秘密鍵を持っているシステム、すなわち、VTR装置5そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

なお、本実施の形態におけるデータ記録再生システムから、図18に示すように、鍵暗号化手段31、鍵暗号解読手段32、鍵暗号解読手段61および鍵暗号化手段63を省略した構成も可能である。こうすれば、本発明のチューナ装置とVTR装置との間のデータ送信において、コンテンツ鍵に暗号化を施さずに送信を行うことになる。以下に、図13の構成のデータ記録再

生システムについて説明する。

図18の構成のデータ記録再生システムにおける、AVデータを記録媒体6に記録する時のデータの流れは、図19に示すようになる。図19において、図18で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図16、図17に倣う。

放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調手段21で復調され、放送用の暗号を放送用デスクランブル手段20で解除され、DMUX23で分離されて、生のAVデータDとなって、映像デコーダ11および音声デコーダ12およびコンテンツ暗号化手段13へ送られる。映像デコーダ11および音声デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、ディスプレイ4へ出力する。コンテンツ暗号化手段13は、コンテンツ鍵Kcoを生成し、生成したコンテンツ鍵Kcoを用いて、AVデータDに暗号化を施して、暗号化AVデータKco(D)を生成する。

暗号化AVデータKco(D)は、D-I/F18を介して、コンテンツ鍵Kcoは、認証鍵交換手段19およびD-I/F18を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換手段19、52は、D-I/F18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

VTR装置5へ伝達された暗号化AVデータKco(D)は、D-I/F51を介して、MUX54へ送られる。また、VTR装置5へ伝達されたコンテンツ鍵Kcoは、D-I/F51および認証鍵交換手段52を介して、

鍵暗号化手段 6 2 に送られる。鍵暗号化手段 6 2 は、VTR 情報記憶手段 7 1 に記憶されている VTR 装置 5 に固有の公開鍵 VTR P a を用いて、コンテンツ鍵 K c o に暗号化を施して、暗号化コンテンツ鍵 VTR P a (K c o) を生成して、これを MUX 5 4 へ送る。MUX 5 4 へ送られた暗号化 AV データ K c o (D) および暗号化コンテンツ鍵 VTR P a (K c o) は、記録媒体 6 のフォーマットに適合した多重化を行われた後、記録処理手段 5 5 によって、記録媒体 6 に記録される。

次に、図 18 の構成のデータ記録再生システムにおける、記録媒体 6 に記録された AV データを再生する時のデータの流れを図 20 を用いて説明する。図 20 において、図 18 で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図 16、図 17 に倣う。

多重化されて記録媒体 6 に記録された暗号化 AV データ K c o (D) および暗号化コンテンツ鍵 VTR P a (K c o) は、再生処理部手段 5 8 により再生され、DMUX 5 7 で分離される。分離された暗号化コンテンツ鍵 VTR P a (K c o) は、鍵暗号解読手段 6 4 へ送られる。鍵暗号解読手段 6 4 は、VTR 情報記憶手段 7 1 に記憶されている VTR 装置 5 に固有の秘密鍵 VTR S a を用いて、暗号化コンテンツ鍵 VTR P a (K c o) をコンテンツ鍵 K c o に復元する。

分離された暗号化 AV データ K c o (D) は、D-I/F 5 1 を介して、復元されたコンテンツ鍵 K c o は、認証鍵交換手段 5 2 および D-I/F 5 1 を介して、それぞれ STB 1 へ伝達されるが、それに先だって、記録時と同様に、STB 1、VTR 装置 5 それぞれの認証鍵交換手段 1 9、5 2 は、D-I/F 1 8 および 5 1 を介して、お互いの認証鍵を交換し、伝達可能な

相手であることを確認した上で、前記伝達が行われる。

STB 1へ伝達された暗号化AVデータKco (D)は、D-I/F 18を介して、コンテンツ暗号解読手段14へ送られ、コンテンツ鍵Kcoは、D-I/F 18および認証鍵交換手段19を介して、それぞれコンテンツ暗号解読手段14へ送られる。コンテンツ暗号解読手段14は、コンテンツ鍵Kcoを用いて、暗号化AVデータKco (D)を解読して得られるAVデータDを、映像デコーダ11および音声デコーダ12へ出力する。映像デコーダ11および音声デコーダ12は、AVデータDに施された高能率符号化处理等をデコードし、ディスプレイ4へ出力する。

なお、STB情報記憶手段17およびVTR情報記憶手段71は、図15の構成において保持していた共通鍵の情報を保持している必要はない。

以上の手順にしたがって、AVデータを記録/再生することにより、STB 1とVTR装置5との間のデータ送信において、コンテンツ鍵に暗号化を施さずに送信を行うので、記録/再生時のSTB 1およびVTR装置5の負担をさらに軽減できるので、図18の構成のデータ記録再生システムは、図15の構成のデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図15の構成のデータ記録再生システムと比較して、STB 1とVTR装置5との間のデータ送信についてのセキュリティは低下する。このような構成は、後述する第8の実施の形態のように、STBおよびVTR装置の機能を一体化した一体化STBを備えるデータ記録再生システムに適用すると、特に有効である。

#### (第7の実施の形態)

以下に、本発明の第7の実施の形態を図面を参照して説明する。本実施の



形態が上述した第1の実施の形態と異なる点は、公開鍵および秘密鍵を用いる替わりに、共通鍵を用いてコンテンツ鍵の暗号化／復元を行う点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

本実施の形態におけるデータ記録再生システムの構成は、第1の実施の形態におけるデータ記録再生システムの構成と同じである。

次に、このような本実施の形態の動作を説明する。

図21は、本発明の第7の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図22は、本発明の第7の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図21、図22に示すとおり、本実施の形態においては、コンテンツ鍵K<sub>co</sub>の暗号化および復元にSTB情報記憶手段17に保持されている共通鍵K<sub>k</sub>を用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。なお、共通鍵K<sub>k</sub>は、例えば、STB1もしくはSTB1の機器モデル、ユーザID、サービスいずれかに対して固有な鍵である。また、共通鍵K<sub>k</sub>は、ICカード2に記録されているとしてもよい。共通鍵K<sub>k</sub>がICカード2に記録されていない場合で、課金情報が、例えば、STB情報記憶手段17に記録される場合は、カード読取手段10を省略してもよい。また、共通鍵K<sub>k</sub>がSTB記憶手段11に記録されていない場合は、STB記憶手段11を省略してもよい。

以上の手順にしたがって、AVデータを記録／再生することにより、コンテンツ鍵に暗号化に公開鍵を用いないので、本実施の形態におけるデータ記

録再生システムは、第1の実施の形態におけるデータ記録再生システムと比較して、鍵自身のデータ長を短くでき、記録効率の向上および装置の小型化を図ることが可能なシステムであることがわかる。

(第8の実施の形態)

以下に、本発明の第8の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、第1の実施の形態におけるデータ記録再生システムが本発明のチューナ装置およびVTR装置を備えていたのに対し、本実施の形態におけるデータ記録再生システムが前記チューナ装置および前記VTR装置の機能が一体化された装置を備えていることに関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

図23は、本発明の第8の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第1の実施の形態におけるデータ記録再生システムの構成と異なるのは、STB1およびVTR装置5の機能を一体化した一体化STB7を備えることによって、第1の実施の形態におけるデータ記録再生システムが備えていたD-I/F18および51を省略したことである。

なお、第1の実施の形態と同様に、課金情報が、例えば、STB情報記憶手段17に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ICカード2およびカード読取手段10を省いてもよい。

次に、このような本実施の形態の動作を説明する。

まず、AVデータを記録媒体6に記録する時のデータの流れを図24を用

いて説明する。図 24 は、本発明の第 8 の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図 24 において、図 23 で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、図 2、図 3 に倣うが、STBPa は、コンテンツ鍵 Kco の暗号化に用いる一体化 STB7 に固有の公開鍵を示す。なお、本実施の形態におけるデータ記録再生システムは、第 1 の実施の形態と同様に、コンテンツ鍵 Kco を、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

放送用電波として暗号化され、多重化された AV データ D は、アンテナ 3 を介して受信され、受信復調手段 21 で復調され、放送用の暗号を放送用デスクランブル手段 20 で解除され、DMUX 23 で分離されて、生の AV データ D となって、映像デコーダ 11 および音声デコーダ 12 およびコンテンツ暗号化手段 13 へ送られる。映像デコーダ 11 および音声デコーダ 12 は、AV データ D に施された高能率符号化処理等をデコードし、ディスプレイ 4 へ出力する。コンテンツ暗号化手段 13 は、コンテンツ鍵 Kco を生成し、生成したコンテンツ鍵 Kco を用いて、AV データ D に暗号化を施して、暗号化 AV データ Kco (D) を生成する。生成されたコンテンツ鍵 Kco は、鍵暗号化手段 15 へ送られ、鍵暗号化手段 15 は、STB 情報記憶手段 17 に記憶されている一体化 STB7 に固有の公開鍵 STBPa を用いて、コンテンツ鍵 Kco に暗号化を施して、暗号化コンテンツ鍵 STBPa (Kco) を生成する。

生成された暗号化 AV データ Kco (D) および暗号化コンテンツ鍵 STB

Pa (Kco) は、それぞれMUX 54へ送られて、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理手段55によって、記録媒体6に記録される。

次に、記録媒体6に記録されたAVデータを再生する時のデータの流れを図25を用いて説明する。図25は、本発明の第8の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図25において、図23で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。図中の記号は、図2、図3に倣うが、STBSaは、公開鍵STBP aに対応し、暗号化コンテンツ鍵 STBP a (Kco) を解読してコンテンツ鍵Kcoを復元するのに用いる一体化STB 7に固有の秘密鍵を示す。

多重化されて記録媒体6に記録された暗号化AVデータKco (D) および暗号化コンテンツ鍵 STBP a (Kco) は、再生処理部手段58により再生され、DMUX 57で分離される。

分離された暗号化AVデータKco (D) は、コンテンツ暗号解読手段14へ送られ、分離された暗号化コンテンツ鍵 STBP a (Kco) は、鍵暗号解読手段16へ送られる。鍵復元手段16は、STB情報記憶手段17に記憶されている一体化STB 7に固有の秘密鍵 STBSaを用いて、暗号化コンテンツ鍵 STBP a (Kco) をコンテンツ鍵Kwに復元して、コンテンツ暗号解読手段14へ送る。コンテンツ暗号解読手段14は、復元されたコンテンツ鍵Kcoを用いて、暗号化AVデータKco (D) を解読して得られるAVデータDを、映像デコーダ11および音声デコーダ12へ出力する。映像デコーダ11および音声デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、ディスプレイ4へ出力する。

以上の手順にしたがって、AVデータを記録／再生することにより、各装置間のデータ伝達にかかる負担を省略できるので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第1の実施の形態におけるデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。

なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、一体化STB7に対して固有な鍵であるとして説明したが、これに限るものではなく、例えば、第2～第4いずれかの実施の形態と同様に、一体化STB7の機器モデルに対して固有な鍵、本発明のICカードに記録されたユーザIDに対して固有な鍵、本発明のICカードに記録されたサービスに対して固有な鍵であってもよい。

なお、本発明のコンテンツ鍵は、上述した第1～第8の実施の形態においては、定期的または不定期的に切り替えられるとして説明したが、同じコンテンツ鍵を用いるとすると、定期的または不定期的に切り替える場合と比較して、暗号化に関する情報が外部に漏洩するおそれが高くなるが、従来のデータ記録再生システムと比較すると、暗号化に関する情報が外部に漏洩しにくいシステムであるといえる。

また、本発明の第2の暗号化は、上述した第1～第8の実施の形態においては、本発明の第1の暗号化において用いたコンテンツ鍵とは別の鍵（公開鍵、共通鍵）であるとして説明したが、これに限るものではなく、第1の暗号化に用いたコンテンツ鍵に対応するアルゴリズムと同じアルゴリズムを用いて、当該コンテンツ鍵自身に第2の暗号化を施すとしてもよい。また、例

例えば、コンテンツ鍵として共通鍵を用いてデジタルデータに第1の暗号化を施し、当該共通鍵に同じ共通鍵を用いて第2の暗号化を施すとしてもよい。なお、上述した第1～第8の実施の形態においては、本発明のデータ記録再生システムを中心に説明したが、本発明のデータ記録再生方法は、上記説明中で、説明された方法である。

#### (第9の実施の形態)

まず、本発明の第9の実施の形態の記録装置および再生装置の構成を述べる。

図26に、本発明の第9の実施の形態の記録装置および再生装置のブロック図を示す。本発明の第9の実施の形態の記録装置は、第1鍵発生手段80と、コンテンツ暗号化手段13と、第2鍵発生手段81と、Kx FIFO 85と、鍵暗号化手段70と、対応関係情報生成手段84と、MUX 54から構成される。また、本発明の第9の実施の形態の再生装置は、DMUX 57と、鍵暗号化鍵取得手段82と、Kxラッチ手段86と、鍵暗号解読手段71と、コンテンツ暗号解読手段14から構成される。なお、図26には、受信復調手段21と、DMUX 23と、EMM解読手段25と、ECM解読手段24と、放送デスクランブル手段20と、映像デコーダ11と、音声デコーダ12も表示する。さらに、記録媒体としての記録媒体6と、映像を表示し、音声を出力するディスプレイ4も表示する。

受信復調手段21は、放送局からの、デジタルの映像データ、音声データ、EMM(個別情報)、ECM(番組情報)および暗号化された放送スクランブル鍵Ksを通信衛星を介して入力し、それらの全部または一部の信号波形を整形する手段である。

さて、DMUX 23は、受信復調手段21からの、波形整形された映像データ、音声データ、EMM、ECMおよび暗号化された放送スクランブル鍵Ksを分離する手段であるとともに、放送デスクランブル手段20からの、デスクランブルされた映像データおよび音声データを分離する手段である。また、DMUX 23は、コンテンツ暗号解読手段14からの映像データおよび音声データを分離する手段でもある。

EMM解読手段25は、ユーザID鍵Kmを入力するとともに、DMUX 23からのEMMを入力し、ユーザID鍵KmでEMMを解読してワーク鍵Kwを生成する手段である。

ECM解読手段24は、EMM解読手段25からのワーク鍵Kwを入力するとともに、DMUX 23からのECMおよび暗号化された放送スクランブル鍵Ksを入力し、ワーク鍵KwでECMを解読して放送スクランブル鍵Ksを復元する手段である。

放送デスクランブル手段20は、ECM解読手段24からの放送スクランブル鍵Ksを入力するとともに、DMUX 23からの、スクランブルされたAVデータを入力し、放送スクランブル鍵Ksで、スクランブルされたAVデータをデスクランブルする手段である。

第1鍵発生手段80は、放送デスクランブル手段20によってデスクランブルされたAVデータを、再度暗号化するためのコンテンツ鍵Kcoを発生する手段である。

コンテンツ暗号化手段13は、放送デスクランブル手段20からのAVデータDを入力するとともに、第1鍵発生手段80からのコンテンツ鍵Kcoを入力し、そのコンテンツ鍵KcoでAVデータDを暗号化する手段である。

なお、以下では、コンテンツ鍵 $K_{co}$ により暗号化されたAVデータ $D$ を $K_{co}(D)$ とする。

第2鍵発生手段81は、第1鍵発生手段80が発生したコンテンツ鍵 $K_{co}$ を暗号化するための鍵暗号化鍵 $K_x$ を発生する手段である。なお、第2鍵発生手段81は、毎日異なる鍵暗号化鍵 $K_x$ を発生するものとし、それら異なる $K_x$ をそれぞれ $K_{x1}$ 、 $K_{x2}$ 、 $K_{x3}$ 、…とする。また、鍵暗号化鍵 $K_{x1}$ 、 $K_{x2}$ 、 $K_{x3}$ 、…それぞれは、1週間で廃棄されるものであるとする。

$K_{x FIFO 85}$ は、第2鍵発生手段81からの鍵暗号化鍵 $K_{x1}$ 、 $K_{x2}$ 、 $K_{x3}$ 、…を入力し格納する手段であるとともに、タイマーを有していて、そのタイマーを利用して、入力後1週間経過した鍵暗号化鍵 $K_x$ を廃棄する、ファーストインファースアウト機能を有する手段である。

鍵暗号化手段70は、第1鍵発生手段80からのコンテンツ鍵 $K_{co}$ を入力するとともに、 $K_{x FIFO 85}$ からの鍵暗号化鍵 $K_x$ を入力し、その鍵暗号化鍵 $K_x$ でコンテンツ鍵 $K_{co}$ を暗号化する手段である。なお、以下では、鍵暗号化鍵 $K_x$ により暗号化されたコンテンツ鍵 $K_{co}$ を $K_x(K_{co})$ とする。

対応関係情報生成手段84は、コンテンツ鍵 $K_{co}$ により暗号化されたAVデータ $K_{co}(D)$ と、そのコンテンツ鍵 $K_{co}$ を暗号化した鍵暗号化鍵 $K_x$ とを対応付けるための情報として、鍵暗号化鍵 $K_x$ 4が発生された日時の情報を生成する手段である。

MUX 54は、コンテンツ暗号化手段13からの暗号化されたAVデータ $K_{co}(D)$ と、鍵暗号化手段70からの $K_x(K_{co})$ と、対応関係情報



生成手段 84 からの日時情報とを入力し、それらを記録媒体 6 に記録する手段である。

DMUX 57 は、記録媒体 6 に記録された、暗号化された AV データ Kc o (D)、Kx (Kc o) および日時情報を入力し、それらを分離する手段である。

鍵暗号化鍵取得手段 82 は、DMUX 57 からの日時情報を入力し、その日時情報に基づいて、再生しようとする暗号化された AV データ Kc o (D) に対応する鍵暗号化鍵 Kx を特定し、その特定した鍵暗号化鍵 Kx を Kx FIFO 85 のなかから取得する手段である。

Kx ラッチ手段 86 は、鍵暗号化鍵取得手段 82 からの鍵暗号化鍵 Kx を入力してラッチし、鍵暗号解読手段 71 に出力する手段である。

鍵暗号解読手段 71 は、DMUX 57 からの Kx (Kc o) を入力するとともに、Kx ラッチ手段 86 からの鍵暗号化鍵 Kx を入力し、その鍵暗号化鍵 Kx で Kx (Kc o) を解読し、コンテンツ鍵 Kc o を復元する手段である。

コンテンツ暗号解読手段 14 は、DMUX 57 からの暗号化された AV データ Kc o (D) を入力するとともに、鍵暗号解読手段 71 からのコンテンツ鍵 Kc o を入力し、そのコンテンツ鍵 Kc o で暗号化された AV データ Kc o (D) を暗号解読する手段である。

映像デコーダ 11 は、DMUX 23 からの映像データを復号する手段である。

音声デコーダ 12 は、DMUX 23 からの音声データを復号する手段である。

なお、請求項 39 の本発明の、コンテンツ暗号化手段としてコンテンツ暗号化手段 13、鍵暗号化鍵発生手段として第 2 鍵発生手段 81、格納手段として K x F I F O 85、鍵暗号化手段として鍵暗号化手段 70、対応関係情報生成手段として対応関係情報生成手段 84、記録手段として MUX 54 を用いた。また、請求項 44 の本発明のコンテンツ鍵発生手段として第 1 鍵発生手段 80 を、本実施の形態では用いた。さらに、請求項 45 の本発明の、鍵暗号化鍵取得手段として鍵暗号化鍵取得手段 82、鍵暗号解読手段として鍵暗号解読手段 71、コンテンツ暗号解読手段としてコンテンツ暗号解読手段 14 を用いた。

次に、このような本発明の第 9 の実施の形態の記録装置の動作を述べる。

まず、受信復調手段 21 は、放送局からの、デジタルの映像データ、音声データ、EMM (個別情報)、ECM (番組情報) および暗号化された放送スクランブル鍵 Ks を入力し、映像データおよび音声データの信号波形の乱れを整形し、映像データ、音声データ、EMM、ECM および暗号化された放送スクランブル鍵 Ks を DMUX 23 に出力する。

その後、DMUX 23 は、受信復調手段 21 からの映像データ、音声データ、EMM、ECM および放送スクランブル鍵 Ks を入力して分離し、映像データおよび音声データ (AV データ) を放送デスクランブル手段 20 に出力する。また、EMM を EMM 解読手段 25 に出力し、ECM および暗号化された放送スクランブル鍵 Ks を ECM 解読手段 24 に出力する。

次に、EMM 解読手段 25 は、ユーザ ID 鍵 Km を入力するとともに、DMUX 23 からの EMM を入力し、ユーザ ID 鍵 Km で EMM を解読してワーク鍵 Kw を生成し、ECM 解読手段 24 に出力する。

さらに、ECM解読手段24は、EMM解読手段25からのワーク鍵Kwを入力するとともに、DMUX23からの、ECMおよび暗号化された放送スクランブル鍵Ksを入力し、ワーク鍵KwでECMを解読して、暗号化された放送スクランブル鍵Ksの暗号化を復元し、放送デスクランブル手段20に出力する。

そして、放送デスクランブル手段20は、ECM解読手段24からの放送スクランブル鍵Ksを入力するとともに、DMUX23からの、スクランブルされたAVデータを入力し、放送スクランブル鍵Ksで、スクランブルされたAVデータをデスクランブルする。そして、放送デスクランブル手段20は、デスクランブルされたAVデータをDMUX23またはコンテンツ暗号化手段13に出力する。なお、放送デスクランブル手段20は、リアルタイムでAVデータを直接ディスプレイ4に表示させる場合にDMUX23に出力し、記録媒体6にAVデータを記録させる場合にコンテンツ暗号化手段13に出力する。ただし、記録媒体6に記録されるAVデータは、放送デスクランブル手段20からの、そのままのAVデータではなく、再度コンテンツ暗号化されたデータである。

はじめに、放送デスクランブル手段20がAVデータをDMUX23に出力する場合について説明する。

その場合、DMUX23は、放送デスクランブル手段20からのAVデータを入力し、それを映像データと音声データに分離して、映像データを映像デコーダ11に出力し、音声データを音声デコーダ12に出力する。その後、映像デコーダ11および音声デコーダ12それぞれは、DMUX23からの映像データまたは音声データを復号し、ディスプレイ4に出力する。そし

て、ディスプレイ 4 は、映像を表示し音声を出力する。

次に、放送デスクランブル手段 20 が AV データをコンテンツ暗号化手段 13 に出力する場合について説明する。つまり、上述したように、記録媒体 6 に AV データを記録する場合である。

まず、コンテンツ暗号化手段 13 は、放送デスクランブル手段 20 からの、デスクランブルされた AV データ D を入力する。

そして、第 1 鍵発生手段 80 は、コンテンツ暗号化手段 13 が入力した AV データ D を暗号化するためのコンテンツ鍵 Kc o を発生し、コンテンツ暗号化手段 13 および鍵暗号化手段 70 に出力する。

次に、コンテンツ暗号化手段 13 は、第 1 鍵発生手段 80 からのコンテンツ鍵 Kc o を入力し、そのコンテンツ鍵 Kc o で AV データ D を暗号化する。つまり、Kc o (D) を生成する。そして、Kc o (D) を対応関係情報生成手段 84 および MUX 54 に出力する。

他方、第 2 鍵発生手段 81 は、第 1 鍵発生手段 80 が発生したコンテンツ鍵 Kc o を暗号化するための鍵暗号化鍵 Kx を発生する。その第 2 鍵発生手段 81 が発生する鍵暗号化鍵 Kx は毎日異なるものとする。ここでは、以下の説明の便宜上、記録装置が動作し始める日を 1998 年 1 月 1 日であるとし、記録時である本日をその日から 3 日後の 1998 年 1 月 4 日であるとし、図 27 の鍵暗号化鍵 Kx リスト (a) に示すように、1 月 1 日に発生された鍵暗号化鍵 Kx を Kx 1、1 月 2 日に発生された鍵暗号化鍵 Kx を Kx 2、…、1 月 4 日に発生された鍵暗号化鍵 Kx を Kx 4 とする。また、以下、同様にして鍵暗号化鍵 Kx は発生されるものとする。なお、ことわりがない限り、以下、1 月 4 日の記録装置の動作について説明する。

さて、K x F I F O 8 5 は、図 2 7 ( a ) のリストに示すように、1 月 1 日から毎日一つづつの鍵暗号化鍵 K x を第 2 鍵発生手段 8 1 から既に入力して格納し、1 月 3 日までに鍵暗号化鍵 K x 1、K x 2、K x 3 を格納しておき、本日 1 月 4 日には、K x 4 を入力して格納する。その格納は、常に最新の鍵暗号化鍵 K x が図 2 7 ( a ) のリストのトップの順位にくるように行われ、また、古いものは順次順位を下げるように行われる。なお、K x F I F O 8 5 は、格納した鍵暗号化鍵 K x 1、K x 2、…を、それぞれの格納から 1 週間経過した後に廃棄する。例えば、図 2 7 ( b ) のリストに示すように、1 月 9 日になると、K x 1、K x 2 という鍵暗号化鍵は廃棄され、K x F I F O 8 5 は、K x 9、K x 8、…、K x 4、K x 3 という順序で 7 つの鍵暗号化鍵を格納することになる。つまり、K x F I F O 8 5 が格納する鍵暗号化鍵 K x の数は 7 までである。

次に、鍵暗号化手段 7 0 は、第 1 鍵発生手段 8 0 からのコンテンツ鍵 K c o を入力するとともに、K x F I F O 8 5 を介して、第 2 鍵発生手段 8 1 が記録時である 1 月 4 日に発生した鍵暗号化鍵 K x 4 を入力し、その鍵暗号化鍵 K x 4 でコンテンツ鍵 K c o を暗号化する。つまり、K x 4 ( K c o ) を生成する。

そして、対応関係情報生成手段 8 4 は、コンテンツ暗号化手段 1 3 からの暗号化された AV データ K c o ( D ) と、鍵暗号化手段 7 0 からの K x 4 ( K c o ) とを入力し、その鍵暗号化鍵 K x 4 と、その鍵暗号化鍵 K x 4 で暗号化されたコンテンツ鍵 K c o により暗号化された AV データ K c o ( D ) とを対応付けるための情報として、その鍵暗号化鍵 K x 4 が発生された日時の情報を生成する。つまり、1 月 4 日という日時情報を生成する。

その後、MUX 54は、コンテンツ暗号化手段13からの暗号化されたAVデータKco (D)と、鍵暗号化手段70からのKx4 (Kco)と、対応関係情報生成手段84からの1月4日という日時情報とを入力し、それらを1組として記録媒体6に記録する。

このようにして、毎日、その日に発生された鍵暗号化鍵Kxn (n=1, 2, ...) に対応するKxn (Kco) と、暗号化されたAVデータKco (D) と、その日の日時情報とが1組となって記録媒体6に記録される。

次に、本発明の第9の実施の形態の再生装置の動作を述べる。

つまり、記録装置によって記録媒体6に記録された暗号化されたAVデータKco (D)を再生する場合について説明する。

以下の説明の便宜上、再生装置が記録媒体6の暗号化されたAVデータKco (D)を再生する日を1月9日であるとする。そして、再生装置は、1月1日に記録媒体6に記録された暗号化されたAVデータKco (D)と、1月3日に記録媒体6に記録された暗号化されたAVデータKco (D)とを再生しようとするものとする。

はじめに、再生装置が1月1日に記録媒体6に記録された暗号化されたAVデータKco (D)を再生しようとする場合について説明する。

まず、DMUX 57は、記録媒体6からの、1月1日に記録された暗号化されたAVデータKco (D)と、Kx1 (Kco)と、1月1日という日時情報とを入力し、それらを分離し、1月1日という日時情報を鍵暗号化鍵取得手段82に出力する。

そして、鍵暗号化鍵取得手段82は、その1月1日という日時情報を入力し、その日時情報に基づいて、鍵暗号化鍵Kx1を特定し、KxFIFO8

5が格納している、図27(b)のリストのなかから鍵暗号化鍵K x 1を検索する。しかしながら、その鍵暗号化鍵K x 1は、発生から一週間以上経過しているため、K x F I F O 8 5により廃棄されており、図27(b)のリストのなかには存在しない。したがって、鍵暗号化鍵取得手段82は、鍵暗号化鍵K x 1を取得することができない。その結果、コンテンツ暗号解読手段14は、その鍵暗号化鍵K x 1を間接的に用いて暗号解読する必要がある、1月1日に記録された暗号化されたAVデータK c o (D)を暗号解読することができなくなり、そのAVデータがディスプレイ4に出力されても、解読不能なため、ディスプレイ4は、AVデータ本来の映像および音声を出力することができない。

次に、再生装置が1月3日に記録媒体6に記録された暗号化されたAVデータK c o (D)を再生しようとする場合について説明する。

まず、DMUX 57は、記録媒体6からの、1月3日に記録された暗号化されたAVデータK c o (D)と、K x 3 (K c o)と、1月3日という日時情報とを入力し、それらを分離し、1月3日という日時情報を鍵暗号化鍵取得手段14に出力する。

次に、鍵暗号化鍵取得手段14は、その1月3日という日時情報を入力し、その日時情報に基づいて、鍵暗号化鍵K x 3を特定し、K x F I F O 8 5が格納している、図27(b)のリストのなかから鍵暗号化鍵K x 3を検索してその鍵暗号化鍵K x 3を取得し、それをK x ラッチ手段86に出力する。

その後、K x ラッチ手段86は、鍵暗号化鍵K x 3を入力し、鍵暗号解読手段71に出力する。また、DMUX 57は、K x 3 (K c o)を鍵暗号解読手段71に出力する。

そして、鍵暗号解読手段 71 は、DMUX 57 からの  $K \times 3$  ( $Kc o$ ) を入力するとともに、 $K \times$  ラッチ手段 86 からの鍵暗号化鍵  $K \times 3$  を入力し、その鍵暗号化鍵  $K \times 3$  で  $K \times 3$  ( $Kc o$ ) を解読し、コンテンツ鍵  $Kc o$  を復元して、そのコンテンツ鍵  $Kc o$  をコンテンツ暗号解読手段 14 に出力する。また、DMUX 57 は、暗号化された AV データ  $Kc o$  (D) を鍵暗号解読手段 71 に出力する。

次に、コンテンツ暗号解読手段 14 は、DMUX 57 からの暗号化された AV データ  $Kc o$  (D) を入力するとともに、鍵暗号解読手段 71 からのコンテンツ鍵  $Kc o$  を入力し、そのコンテンツ鍵  $Kc o$  で暗号化された AV データ  $Kc o$  (D) を暗号解読して、その暗号解読された AV データを DMUX 23 に出力する。

そして、DMUX 23 は、コンテンツ暗号解読手段 14 からの AV データ D を入力し、それを映像データと音声データに分離して、映像データを映像デコーダ 11 に出力し、音声データを音声デコーダ 12 に出力する。その後、映像デコーダ 11 および音声デコーダ 12 それぞれは、DMUX 23 からの映像データまたは音声データを復号し、ディスプレイ 4 に出力する。そして、ディスプレイ 4 は、映像を表示し音声を出力する。

このようにして、記録媒体 6 に記録された暗号化された AV データ  $Kc o$  (D) それぞれは、記録されてから 1 週間以内でないと、最終的に、本来の映像および音声として再生されない。

なお、上述した第 9 の実施の形態では、記録媒体 6 に記録された暗号化された AV データ  $Kc o$  (D) それぞれは、記録されてから 1 週間以内であれば再生されたとしたが、1 週間以内というような期間の制限ではなく、暗号



化されたAVデータKco(D)それぞれの再生回数を、例えば1回や3回というように制限して、その制限再生回数内でないと、再生されないとしてもよい。つまり、図28に示すように、本発明の再生装置がカウンタ87を備え、そのカウンタ87が各暗号化されたAVデータKco(D)の再生回数をチェックし、例えば1回や3回というような制限された再生回数に達した場合、KxFIFO85が、その暗号化されたAVデータKco(D)に対応する鍵暗号化鍵Kxを廃棄するとしてもよい。また、上述した1週間以内というような期間の制限と再生回数の制限を併用するとしてもよい。

また、上述した第9の実施の形態では、KxFIFO85は、格納した鍵暗号化鍵Kxを1週間経過した後には廃棄するとした。しかし、KxFIFO85は、格納した鍵暗号化鍵Kxを1週間経過しても廃棄せずに、格納したままにしておき、鍵暗号化鍵取得手段82が、暗号化されたAVデータKco(D)を再生しようとする日が鍵暗号化鍵Kxの発生から1週間以内か否かを判断して、または、制限回数内か否かを判断して、1週間以内または制限回数内以内であれば、再生しようとする暗号化されたAVデータKco(D)に対応する鍵暗号化鍵KxをKxFIFO85から取得できるとしてもよい。したがって、この場合、請求項46の本発明では、コンテンツ暗号化手段としてコンテンツ暗号化手段13、鍵暗号化鍵発生手段として第2鍵発生手段81、格納手段としてKxFIFO85、鍵暗号化手段として鍵暗号化手段70、対応関係情報生成手段として対応関係情報生成手段84、記録手段としてMUX54がそれぞれ該当することになる。また、請求項50の本発明では、鍵暗号化鍵取得手段として鍵暗号化鍵取得手段82、鍵暗号解読手段として鍵暗号解読手段71、コンテンツ暗号解読手段としてコンテン

ツ暗号解読手段14がそれぞれ該当することになる。

また、上述した第9の実施の形態では、第1鍵発生手段80は、コンテンツ暗号化手段13が入力したAVデータDを暗号化するためのコンテンツ鍵Kcoを発生するとした。しかし、本発明の記録装置は、図29に示すように、第1鍵発生手段80を備えず、コンテンツ暗号化手段13は、放送局から送られてくる放送スクランブル鍵Ksを、放送デスクランブル手段20を介して入力し、その放送スクランブル鍵Ksで、または、その放送スクランブル鍵Ksを加工したもので、AVデータDを暗号化するとしてもよい。その場合、鍵暗号化手段70は、コンテンツ暗号化手段13から、放送スクランブル鍵Ks、または、その放送スクランブル鍵Ksを加工したものを入力し、それを鍵暗号化鍵Kxで暗号化する。

また、上述した第9の実施の形態では、コンテンツ暗号化手段13は、第1鍵発生手段80からのコンテンツ鍵KcoでAVデータDを暗号化するとした。しかし、本発明の記録装置は、図30に示すように、第1鍵発生手段80、鍵暗号化手段15を備えず、コンテンツ暗号化手段13は、第2鍵発生手段81からの鍵暗号化鍵KxをKxFIFO85を介して入力し、その鍵暗号化鍵Kxをコンテンツ鍵Kxとして使用し、そのコンテンツ鍵Kxにより、AVデータDを暗号化するとしてもよい。この場合、記録媒体6には、コンテンツ鍵Kxにより暗号化されたAVデータD、つまり、Kx(AVデータ)と、コンテンツ鍵Kxとが記録される。またその場合、本発明の再生装置は、図30に示すように、鍵復元手段16を備えないことになる。したがって、Kx(AVデータ)を再生しようとする場合、コンテンツ鍵取得手段83は、対応するコンテンツ鍵Kxを特定し、それをKxFIFO85

のなかから取得する。そして、コンテンツ暗号解読手段14は、記録媒体6からのKx(AVデータ)をDMUX57を介して入力するとともに、鍵暗号化鍵取得手段82からのコンテンツ鍵KxをKxラッチ手段86を介して入力し、そのコンテンツ鍵KxでKx(AVデータ)を暗号解読する。そのため、この場合、つまり、請求項53および20の本発明では、コンテンツ鍵発生手段として第2鍵発生手段81、格納手段としてKx FIFO85、コンテンツ暗号化手段としてコンテンツ暗号化手段13、対応関係情報生成手段として対応関係情報生成手段84、記録手段としてDMUX23がそれぞれ該当することになる。また、請求項57および22の本発明では、コンテンツ鍵取得手段としてコンテンツ鍵取得手段83、コンテンツ暗号解読手段としてコンテンツ暗号解読手段14がそれぞれ該当することになる。

また、上述した第9の実施の形態の記録装置は、図31に示すように、課金手段88を備え、記録媒体6に暗号化されたAVデータKco(D)を記録するさい、その記録に対する所定の課金をユーザに課し、あらかじめユーザから所定の料金が放送局等に支払われた場合、もしくは、少なくとも記録するさいに所定の料金が支払われた場合のみ、暗号化されたAVデータKco(D)は記録媒体6に記録されるとしてもよい。また、課金手段88は、図31に示す位置に配置されなくとも、鍵暗号化手段15とMUX54との間に配置されるとしてもよい。要するに、課金手段88は、記録媒体6に暗号化されたAVデータKco(D)を記録するさい、その記録に対する所定の課金をユーザに課すものでありさえすればよく、配置場所はどの場所であってもよい。

また、上述した第9の実施の形態では、鍵暗号化鍵Kxそれぞれは、発生

から1週間経過すると廃棄されるとしたが、廃棄される日時は、発生から1週間経過後に限定することではなく、1日経過後であっても、3日経過後であっても、または、12時間経過後であってもよい。要するに、鍵暗号化鍵Kxそれぞれは、発生から所定の期間経過すると廃棄されさえすればよい。

また、上述した第9の実施の形態では、第2鍵発生手段81は、毎日、1つつ異なる鍵暗号化鍵Kxを発生するとしたが、第2鍵発生手段81は、同じ日であっても、数時間毎に異なる鍵暗号化鍵Kxを発生するとしてもよい。さらに、記録媒体6に所定の番組の暗号化されたAVデータKco(D)を記録する毎に鍵暗号化鍵Kxを発生するとしてもよい。つまり、一回の記録開始からその記録の終了毎に、その都度、鍵暗号化鍵Kxを発生するとしてもよい。要するに、第2鍵発生手段81は、記録しようとする暗号化されたAVデータKco(D)のコンテンツ鍵Kcoを暗号化するための鍵暗号化鍵Kxを発生しさえすればよい。

また、上述した第9の実施の形態では、本発明の対応関係情報として、鍵暗号化鍵Kxが発生されたさいの日時情報を用いたが、本発明の対応関係情報は、コンテンツ暗号化手段13がAVデータDを入力した日時、コンテンツ暗号化手段13がコンテンツ鍵KcoでAVデータDをコンテンツ暗号化した日時、第2鍵発生手段81が鍵暗号化鍵Kxを発生した日時、KxFI F085が鍵暗号化鍵Kxを格納した日時、鍵暗号化手段70が鍵暗号化鍵Kxでコンテンツ鍵Kcoを暗号化した日時、または、MUX54が記録媒体6に暗号化されたAVデータKco(D)を記録した日時の情報であってもよい。もしくは、上述した鍵暗号化鍵Kxが発生されたさいの日時や、コンテンツ暗号化手段13がAVデータDを入力した日時等と、AVデータを

再生しようとする日時との情報であってもよい。その場合、図 27 の鍵暗号化鍵 K x リストの各鍵暗号化鍵 K x が毎日順位を下げることに基づいて、また、2 つの日時の差が考慮されて、鍵暗号化鍵 K x が取得されることになる。または、本発明の対応関係情報は、上述した鍵暗号化鍵 K x が発生されたさいの日時や、コンテンツ暗号化手段 13 が AV データ D を入力した日時等と、AV データを再生しようとする日時とに基づき、また、図 27 の鍵暗号化鍵 K x リストの各鍵暗号化鍵 K x が毎日順位を下げるのが考慮された、図 27 の鍵暗号化鍵 K x リストの番号情報等であってもよい。

また、上述した第 9 の実施の形態では、記録媒体としての記録媒体 6 を用いたが、記録媒体は、記録媒体 6 に限らず、ハードディスクであってもよい。

また、上述した第 9 の実施の形態では、第 1 鍵発生手段 80 は AV データ D を暗号化するためのコンテンツ鍵 K c o を発生するが、そのコンテンツ鍵 K c o は、簡単に解読することができないように、例えば数十秒などの短い期間で更新されるとしてもよい。

さらに、上述した記録装置または再生装置は、鍵暗号化鍵 K x の発生から例えば 1 週間という所定の期間を経過するなどして、その鍵暗号化鍵 K x が廃棄されたり、使用不可になる前に、その鍵暗号化鍵 K x に対応する暗号化された AV データ K c o (D) が一度も再生されていない場合、その旨の情報をユーザに通知する手段を備えてもよい。

#### 産業上の利用可能性

以上説明したところから明らかなように、請求項 1 の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、

前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法を提供することができる。また、請求項4の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムを提供することができる。また、請求項22または23の本発明は、記録および／または再生時に、確実に課金が可能なデータ記録再生方法およびデータ記録再生システムを提供することができる。さらに、請求項30の本発明は、再生時のロスタイムが少ないデータ記録再生システムを提供することができる。

さらに、本発明は、AVデータを記録媒体に記録し、そのAVデータの有効再生期間や有効再生回数の制限を遵守する記録装置および再生装置を提供することができる。

なお、本発明のプログラム媒体は、上述した発明の各構成要素の全部又は一部をコンピュータで実現するためのプログラムを格納したことを特徴とするCD-ROM等のプログラム媒体である。

## 請 求 の 範 囲

1. デジタルデータにコンテンツ鍵を用いて第1の暗号化を施した暗号化デジタルデータと、前記コンテンツ鍵に第2の暗号化を施した暗号化コンテンツ鍵とを記録媒体に記録し、記録された前記暗号化デジタルデータおよび前記暗号化コンテンツ鍵を再生し、前記暗号化コンテンツ鍵を解読して得られた前記コンテンツ鍵を用いて前記暗号化デジタルデータを解読して、前記デジタルデータを得ることを特徴とするデータ記録再生方法。
2. 前記暗号化コンテンツ鍵を、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項1に記載のデータ記録再生方法。
3. 前記コンテンツ鍵を、定期的または不定期的に切り替えることを特徴とする請求項1または2に記載のデータ記録再生方法。
4. デジタルデータを入力するとともに、前記デジタルデータを暗号化するためのコンテンツ鍵を入力し、そのコンテンツ鍵を用いて前記デジタルデータに第1の暗号化を施して暗号化デジタルデータを生成するコンテンツ暗号化手段と、前記コンテンツ鍵に第2の暗号化を施して暗号化コンテンツ鍵を生成する鍵暗号化手段と、前記暗号化デジタルデータおよび前記暗号化コンテンツ鍵を記録媒体に記録する記録手段と、前記記録媒体から前記暗号化デジタルデータおよび前記暗号化コンテンツ鍵を再生する再生手段と、前記暗号化コンテンツ鍵を解読して前記コンテンツ鍵を復元する鍵暗号解読手段と、復元された前記コンテンツ鍵を用いて前記暗号化デジタルデータを解読して、前記デジタルデータを得るコンテンツ暗号解読手段とを備えることを特徴とするデータ記録再生システム。
5. 前記全ての手段は、一体化された装置に備えられていることを特徴

とする請求項 4 に記載のデータ記録再生システム。

6. 前記受信手段と、前記コンテンツ暗号化手段と、前記コンテンツ暗号解読手段とは、チューナ装置に備えられ、前記記録手段と、前記再生手段とは、VTR装置に備えられていることを特徴とする請求項 4 に記載のデータ記録再生システム。

7. 前記第 2 の暗号化は、公開鍵を用いて施され、前記暗号化コンテンツ鍵の解読は、前記公開鍵に対応する秘密鍵を用いて施されることを特徴とする請求項 6 に記載のデータ記録再生システム。

8. 前記鍵暗号解読手段は、前記チューナ装置に備えられていることを特徴とする請求項 7 に記載のデータ記録再生システム。

9. 前記公開鍵および前記秘密鍵は、前記チューナ装置に対して固有な鍵であることを特徴とする請求項 8 に記載のデータ記録再生システム。

10. 前記公開鍵および前記秘密鍵は、前記チューナ装置の機器モデルに対して固有な鍵であることを特徴とする請求項 8 に記載のデータ記録再生システム。

11. 前記チューナ装置は、ICカードに記録された情報を読み取るカード読取手段を有することを特徴とする請求項 8 に記載のデータ記録再生システム。

12. 前記公開鍵および前記秘密鍵は、前記ICカードに記録されたユーザIDに対して固有な鍵であることを特徴とする請求項 11 に記載のデータ記録再生システム。

13. 前記公開鍵および前記秘密鍵は、前記ICカードに記録されたサービスに対して固有な鍵であることを特徴とする請求項 11 に記載のデータ



記録再生システム。

14. 前記ICカードには、前記ユーザIDに対して固有な鍵に加えて、少なくとも一つの別のユーザIDに対して固有な公開鍵が記録されており、前記鍵暗号化手段は、前記第2の暗号化とともに、前記別のユーザIDに対して固有な公開鍵を用いて、前記コンテンツ鍵を暗号化して、前記別のユーザIDに対して固有な公開鍵毎に、別の暗号化コンテンツ鍵を生成し、前記記録手段は、前記暗号化コンテンツ鍵に加えて、前記別の暗号化コンテンツ鍵も前記記録媒体に記録することを特徴とする請求項12に記載のデータ記録再生システム。

15. 前記鍵暗号化手段は、前記チューナ装置または前記VTR装置のいずれかに備えられていることを特徴とする請求項8～14のいずれかに記載のデータ記録再生システム。

16. 前記鍵暗号化手段が前記VTR装置に備えられている場合は、前記チューナ装置は、前記コンテンツ鍵を共通鍵によって暗号化する第二の鍵暗号化手段を有し、前記VTR装置は、前記共通鍵によって暗号化された前記コンテンツ鍵を解読する第二の鍵暗号解読手段を有することを特徴とする請求項15に記載のデータ記録再生システム。

17. 前記公開鍵および前記秘密鍵は、前記VTR装置に対して固有な鍵であり、前記鍵暗号化手段および前記鍵暗号解読手段は、前記VTR装置に備えられていることを特徴とする請求項7に記載のデータ記録再生システム。

18. 前記チューナ装置は、前記コンテンツ鍵を共通鍵によって暗号化する第二の鍵暗号化手段と、前記共通鍵によって暗号化された前記コンテン

ツ鍵を解読する第二の鍵暗号解読手段とを有し、前記VTR装置は、前記コンテンツ鍵を前記共通鍵によって暗号化する第三の鍵暗号化手段と、前記共通鍵によって暗号化された前記コンテンツ鍵を解読する第三の鍵暗号解読手段とを有し、前記第三の鍵暗号解読手段は、前記第二の鍵暗号化手段により暗号化された前記コンテンツ鍵を解読し、前記第二の鍵暗号解読手段は、前記第三の鍵暗号化手段により暗号化された前記コンテンツ鍵を解読することを特徴とする請求項17に記載のデータ記録再生システム。

19. 前記第2の暗号化および前記暗号化コンテンツ鍵の解読は、共通鍵を用いて施され、前記鍵暗号化手段および前記鍵暗号解読手段は、前記チューナ装置に備えられていることを特徴とする請求項6に記載のデータ記録再生システム。

20. 前記共通鍵は、前記チューナ装置、もしくは、前記チューナ装置の機器モデルに対して固有な鍵であることを特徴とする請求項19に記載のデータ記録再生システム。

21. 前記チューナ装置は、ICカードに記録された情報を読み取るカード読取手段を有し、前記共通鍵は、前記ICカードに記録されたユーザID、もしくは、前記ICカードに記録されたサービスに対して固有な鍵に対して固有な鍵であることを特徴とする請求項19に記載のデータ記録再生システム。

22. 前記チューナ装置は、前記記録媒体の記録時に課金情報を生成し、それを記憶することを特徴とする請求項6～21のいずれかに記載のデータ記録再生システム。

23. 前記チューナ装置は、前記記録媒体の再生時に課金情報を生成し

、それを記憶することを特徴とする請求項 6～21 のいずれかに記載のデータ記録再生システム。

24. 前記記録媒体の記録時に、前記課金情報を生成するために必要な情報を、前記記録媒体に記録し、前記記録媒体の再生時に前記必要な情報を用いて前記課金情報を生成することを特徴とする請求項 23 に記載のデータ記録再生システム。

25. 前記課金情報は、前記記録媒体の再生期間の限定を伴うものであることを特徴とする請求項 23 または 24 に記載のデータ記録再生システム。

26. 前記課金情報は、前記記録媒体の再生回数の限定を伴うものであることを特徴とする請求項 23～25 のいずれかに記載のデータ記録再生システム。

27. 前記チューナ装置は、前記 IC カードに前記課金情報を記憶させることを特徴とする請求項 22～26 のいずれかに記載のデータ記録再生システム。

28. 前記チューナ装置は、前記課金情報をサービスプロバイダに対して、通信を介して、出力することを特徴とする請求項 22～27 のいずれかに記載のデータ記録再生システム。

29. 前記暗号化コンテンツ鍵を、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項 4～28 のいずれかに記載のデータ記録再生システム。

30. 前記第 2 の暗号化を施した鍵の固有性に関する情報を、前記記録媒体に記録することを特徴とする請求項 4～29 のいずれかに記載のデータ記録再生システム。

31. 前記コンテンツ鍵を、定期的または不定期的に切り替えることを特徴とする請求項4～30のいずれかに記載のデータ記録再生システム。

32. 前記切り替えの後のコンテンツ鍵に対応する前記暗号化コンテンツ鍵が、前記切り替えの前のコンテンツ鍵に対応する前記暗号化デジタルデータの少なくとも一部とタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項31に記載のデータ記録再生システム。

33. 一つの前記コンテンツ鍵に対応する前記暗号化コンテンツ鍵が、それに対応する前記暗号化デジタルデータとタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項31または32に記載のデータ記録再生システム。

34. 前記チューナ装置を備える場合は、前記チューナ装置が前記切り替えを行うことを特徴とする請求項31～33のいずれかに記載のデータ記録再生システム。

35. 前記VTR装置を備える場合は、前記VTR装置が、前記切り替えに対応して、前記暗号化コンテンツ鍵の再生のタイミングを決定することを特徴とする請求項31～34のいずれかに記載のデータ記録再生システム。

36. 前記暗号化デジタルデータおよび前記暗号化コンテンツ鍵は、前記記録媒体上の前記再生のタイミングに対応する記録位置に、記録されることを特徴とする請求項31～35のいずれかに記載のデータ記録再生システム。

37. 前記切り替えのタイミングも合わせて、前記記録媒体に記録することを特徴とする請求項36に記載のデータ記録再生システム。

38. 前記チューナ装置および前記VTR装置を備える場合は、前記V

TR装置が、前記切り替えの後のコンテンツ鍵、もしくは、それに対応する前記暗号化コンテンツ鍵を、前記切り替えの後のコンテンツ鍵に対応する前記暗号化デジタルデータの出力より前もって、前記チューナ装置へ出力することを特徴とする請求項31～37のいずれかに記載のデータ記録再生システム。

39. デジタルデータを入力するとともに、前記デジタルデータを暗号化するためのコンテンツ鍵を入力し、そのコンテンツ鍵を用いて前記デジタルデータに第1の暗号化を施して暗号化デジタルデータを生成するコンテンツ暗号化手段と、

前記コンテンツ鍵に第2の暗号化を施すための鍵暗号化鍵を発生する鍵暗号化鍵発生手段と、前記鍵暗号化鍵を格納し、その後、その鍵暗号化鍵が所定の条件に合えば、その鍵暗号化鍵を消去する格納手段と、

前記鍵暗号化鍵で前記コンテンツ鍵に第2の暗号化を施して暗号化コンテンツ鍵を生成する鍵暗号化手段と、

前記コンテンツ鍵により暗号化した暗号化デジタルデータと、そのコンテンツ鍵を暗号化した鍵暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記暗号化デジタルデータ、前記暗号化コンテンツ鍵、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする記録装置。

40. 前記所定の条件とは、前記鍵暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項39記載の記録装置。

4 1. 前記対応関係情報とは、前記コンテンツ暗号化手段が前記デジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で前記デジタルデータを暗号化した日時、前記鍵暗号化鍵発生手段が前記鍵暗号化鍵を発生した日時、前記格納手段が前記鍵暗号化鍵を格納した日時、前記鍵暗号化手段が前記鍵暗号化鍵で前記コンテンツ鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化デジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項 3 9 または 4 0 記載の記録装置。

4 2. 前記所定の条件とは、前記暗号化デジタルデータの再生のさいに、前記鍵暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項 3 9 記載の記録装置。

4 3. 前記コンテンツ鍵を発生するコンテンツ鍵発生手段を備え、前記コンテンツ暗号化手段は、前記コンテンツ鍵発生手段から前記コンテンツ鍵を入力することを特徴とする請求項 3 9 から 4 2 のいずれかに記載の記録装置。

4 4. 前記コンテンツ暗号化手段は、放送局からの前記コンテンツ鍵を入力し、そのコンテンツ鍵を利用することを特徴とする請求項 3 9 から 4 2 のいずれかに記載の記録装置。

4 5. 請求項 3 9 から 4 4 のいずれかに記載の記録装置における前記記録媒体上の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化デジタルデータに対応する鍵暗号化鍵を特定し、前記記録装置における前記格納手段のなかの前記鍵暗号化鍵を検索して取得する鍵暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとする暗号化デジタルデー

タに対応する、暗号化されたコンテンツ鍵を入力するとともに、前記鍵暗号化鍵を入力し、その鍵暗号化鍵で前記暗号化されたコンテンツ鍵の暗号化を解く鍵暗号解読手段と、

前記鍵暗号解読手段からのコンテンツ鍵で前記暗号化デジタルデータの暗号化を解読するコンテンツ暗号解読手段とを

備えたことを特徴とする再生装置。

46. デジタルデータを入力するとともに、前記デジタルデータを暗号化するためのコンテンツ鍵を入力し、そのコンテンツ鍵で前記デジタルデータに第1の暗号化を施し暗号化デジタルデータを生成するコンテンツ暗号化手段と、

前記コンテンツ鍵に第2の暗号化を施すための鍵暗号化鍵を発生する鍵暗号化鍵発生手段と、

前記鍵暗号化鍵発生手段が発生した鍵暗号化鍵を格納する格納手段と、

前記鍵暗号化鍵で前記コンテンツ鍵を暗号化する鍵暗号化手段と、

前記コンテンツ鍵により暗号化された暗号化デジタルデータと、そのコンテンツ鍵を暗号化した鍵暗号化鍵との対応関係情報を生成する対応関係情報生成手段と、

前記暗号化デジタルデータ、前記暗号化コンテンツ鍵、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする記録装置。

47. 前記対応関係情報とは、前記コンテンツ暗号化手段が前記デジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で

前記デジタルデータを暗号化した日時、前記鍵暗号化鍵発生手段が前記鍵暗号化鍵を発生した日時、前記格納手段が前記鍵暗号化鍵を格納した日時、前記鍵暗号化手段が前記鍵暗号化鍵で前記コンテンツ鍵を暗号化した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化デジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項 4、6 記載の記録装置。

48. 前記コンテンツ鍵を発生するコンテンツ鍵発生手段を備え、前記コンテンツ暗号化手段は、前記コンテンツ鍵発生手段から前記コンテンツ鍵を入力することを特徴とする請求項 4、6 または 47 記載の記録装置。

49. 前記コンテンツ暗号化手段は、放送局からの前記コンテンツ鍵を入力し、そのコンテンツ鍵を利用することを特徴とする請求項 4、6 または 47 記載の記録装置。

50. 請求項 4、6 から 49 のいずれかに記載の記録装置における前記記録媒体上の対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化デジタルデータに対応する鍵暗号化鍵を特定し、さらに、その鍵暗号化鍵が所定の条件に合うかどうかを判定し、合致する場合は、その鍵暗号化鍵を、前記記録装置における前記格納手段から取り出し、合致しない場合は、その鍵暗号化鍵を前記格納手段から取り出さない鍵暗号化鍵取得手段と、

前記所定の記録媒体からの、前記再生しようとする暗号化デジタルデータに対応する、暗号化されたコンテンツ鍵を入力するとともに、前記鍵暗号化鍵を入力し、その鍵暗号化鍵で前記暗号化されたコンテンツ鍵の暗号化を解いてコンテンツ鍵を復元する鍵暗号解読手段と、



前記鍵暗号解読手段からのコンテンツ鍵で前記暗号化デジタルデータの暗号化を解読するコンテンツ暗号解読手段とを

備えたことを特徴とする再生装置。

51. 前記所定の条件とは、請求項46から49のいずれかに記載の記録装置の前記格納手段に、前記鍵暗号化鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項50記載の再生装置。

52. 前記所定の条件とは、前記暗号化デジタルデータの再生のさいに、前記鍵暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項50記載の再生装置。

53. デジタルデータを暗号化するためのコンテンツ鍵を発生するコンテンツ鍵発生手段と、

前記コンテンツ鍵発生手段が発生したコンテンツ鍵を格納し、その後、そのコンテンツ鍵が所定の条件に合えば、そのコンテンツ鍵を消去する格納手段と、

前記コンテンツ鍵で前記デジタルデータを暗号化するコンテンツ暗号化手段と、

前記コンテンツ鍵により暗号化された暗号化デジタルデータと、そのコンテンツ鍵との対応関係情報を生成する対応関係情報生成手段と、前記暗号化デジタルデータ、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを

備えたことを特徴とする記録装置。

54. 前記所定の条件とは、前記コンテンツ鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項53記載の記録装置。

55. 前記対応関係情報とは、前記コンテンツ暗号化手段が前記デジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で前記デジタルデータを暗号化した日時、前記コンテンツ鍵発生手段が前記コンテンツ鍵を発生した日時、前記格納手段が前記コンテンツ鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化デジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項53または54記載の記録装置。

56. 前記所定の条件とは、前記暗号化デジタルデータの再生のさいに、前記鍵暗号化鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項53記載の記録装置。

57. 請求項53から56のいずれかに記載の記録装置の前記記録媒体上の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化デジタルデータに対応するコンテンツ鍵を特定し、前記記録装置の前記格納手段のなかの前記コンテンツ鍵を検索して取得するコンテンツ鍵取得手段と、

前記所定の記録媒体から前記暗号化デジタルデータを入力するとともに、前記コンテンツ鍵を入力し、そのコンテンツ鍵で前記暗号化デジタルデータの暗号化を解読するコンテンツ暗号解読手段とを備えたことを特徴とする再生装置。

58. デジタルデータを暗号化するためのコンテンツ鍵を発生するコンテンツ鍵発生手段と、

前記コンテンツ鍵発生手段が発生したコンテンツ鍵を格納する格納手段と

前記コンテンツ鍵で前記デジタルデータを暗号化して暗号化デジタルデータを取得するコンテンツ暗号化手段と、

前記コンテンツ鍵により暗号化された暗号化デジタルデータと、そのコンテンツ鍵との対応関係情報を生成する対応関係情報生成手段と、前記暗号化デジタルデータ、および、前記対応関係情報の全部または一部を入力し、それらを所定の記録媒体に記録する記録手段とを備えたことを特徴とする記録装置。

59. 前記対応関係情報とは、前記コンテンツ暗号化手段が前記デジタルデータを入力した日時、前記コンテンツ暗号化手段が前記コンテンツ鍵で前記デジタルデータをコンテンツ暗号化した日時、前記コンテンツ鍵発生手段が前記コンテンツ鍵を発生した日時、前記格納手段が前記コンテンツ鍵を格納した日時、または、前記記録手段が前記所定の記録媒体に前記暗号化デジタルデータを記録した日時で対応付けられた情報であることを特徴とする請求項58記載の記録装置。

60. 請求項58または59記載の記録装置の前記記録媒体上の前記対応関係情報を入力し、その対応関係情報に基づいて、再生しようとする暗号化デジタルデータに対応するコンテンツ鍵を特定し、さらに、そのコンテンツ鍵が所定の条件に合うかどうかを判定し、合致する場合は、そのコンテンツ鍵を、前記記録装置の前記格納手段から取り出し、合致しない場合は、そのコンテンツ鍵を前記格納手段から取り出さないコンテンツ鍵取得手段と、前記コンテンツ鍵で前記暗号化デジタルデータの暗号化を解読するコンテンツ暗号解読手段とを

備えたことを特徴とする再生装置。

61. 前記所定の条件とは、請求項58または59記載の記録装置の前記格納手段に、前記コンテンツ鍵が格納された後、所定の時間を超えることを意味することを特徴とする請求項60記載の再生装置。

62. 前記所定の条件とは、前記暗号化デジタルデータの再生のさいに、前記コンテンツ鍵の利用された回数が、所定の回数を超えることを意味することを特徴とする請求項60記載の再生装置。

63. 前記記録手段が前記暗号化デジタルデータを、前記所定の記録媒体に記録するさい、前記データの記録に対する課金を課す課金手段を備えたことを特徴とする請求項39から44のいずれか、または、請求項46から49のいずれか、または、請求項53から56のいずれか、または、請求項58から59のいずれかに記載の記録装置。

64. 前記所定の記録媒体は、ビデオテープであることを特徴とする請求項39から44のいずれか、または、請求項46から49のいずれか、または、請求項53から56のいずれか、または、請求項58から59のいずれかに記載の記録装置。

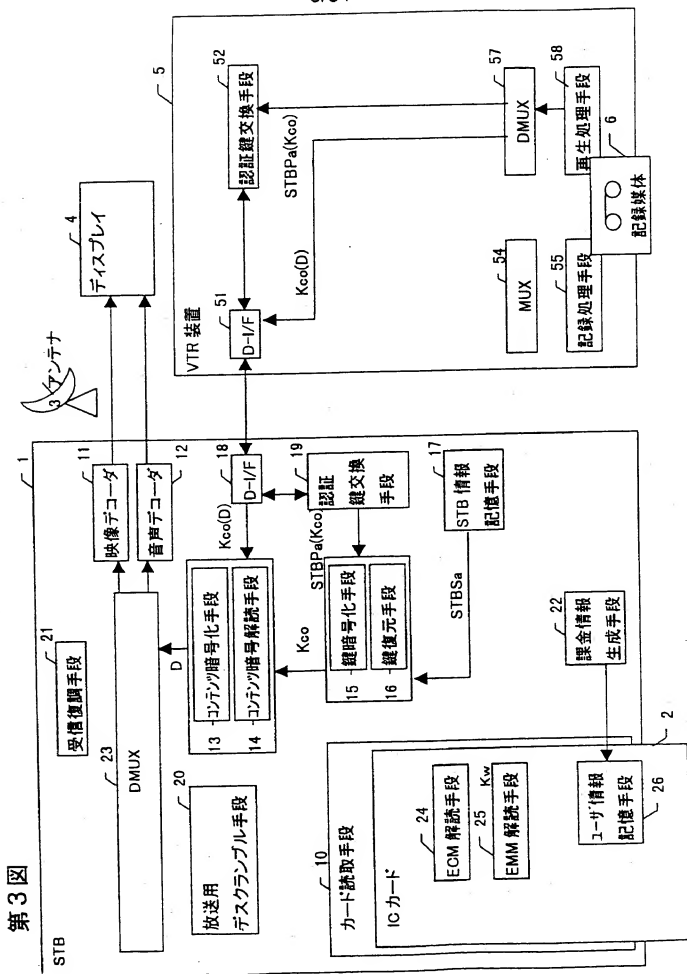
65. 前記所定の記録媒体は、ハードディスクであることを特徴とする請求項39から44のいずれか、または、請求項46から49のいずれか、または、請求項53から56のいずれか、または、請求項58から59のいずれかに記載の記録装置。

66. 請求項1～65のいずれかに記載の請求項における各構成要素の全部又は一部をコンピュータで実現するためのプログラムを格納したことを特徴とするプログラム媒体。





3/31



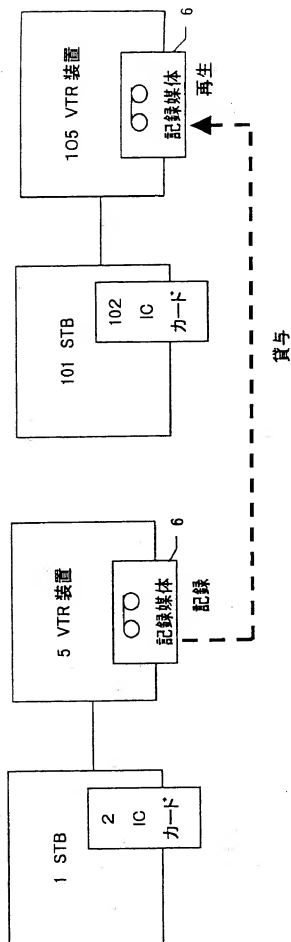
4/31

第4図

メインエリア	暗号化 AVデータ	Kco-a(D)		Kco-b(D)		Kco-c(D)		Kco-d(D)	
サブエリア	次の コンテンツ鍵	Kco-b		Kco-c		Kco-d		Kco-e	
サブエリア	現在の コンテンツ鍵	Kco-a		Kco-b		Kco-c		Kco-d	
→ 時間									

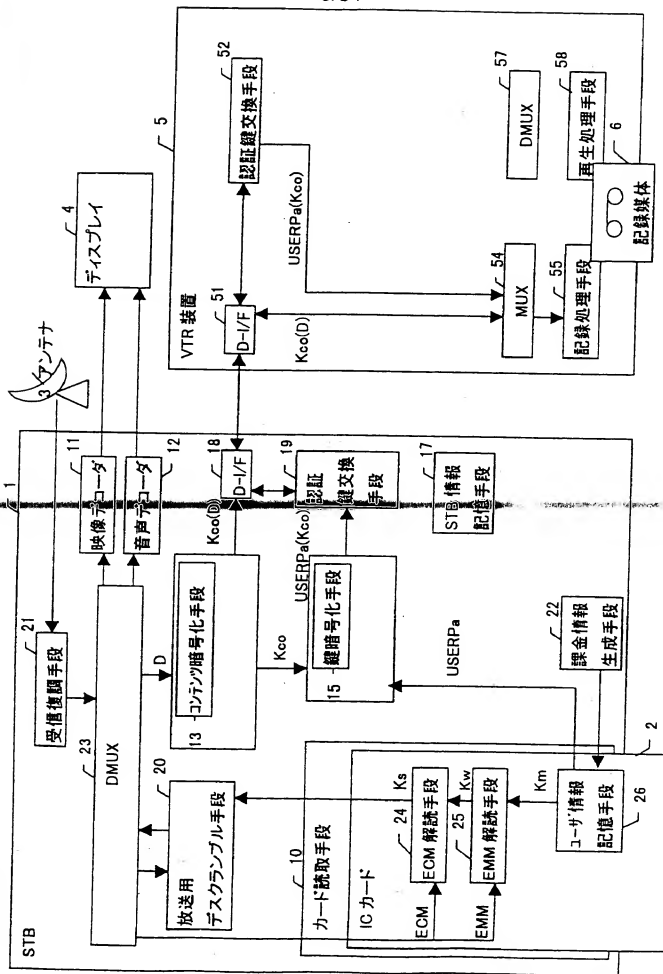


5/31



第5図

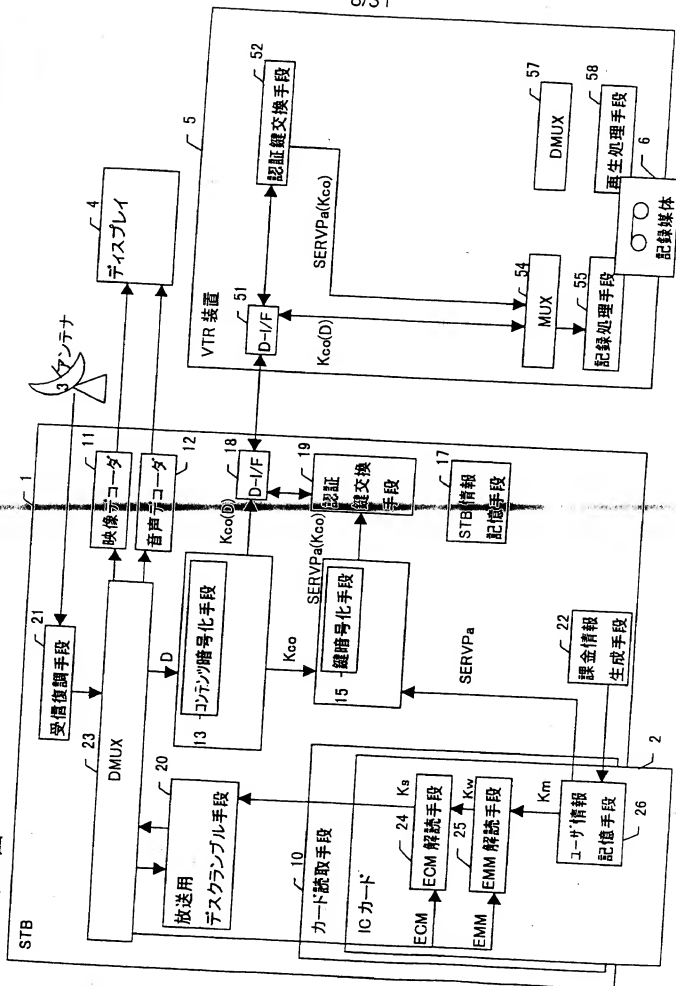
第6図





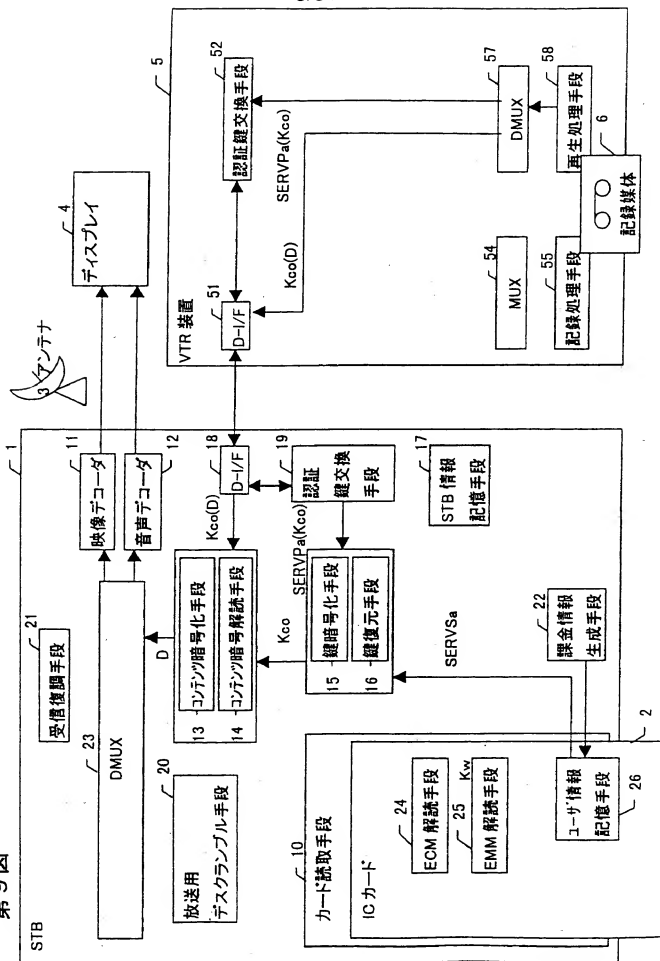
8/31

第8図



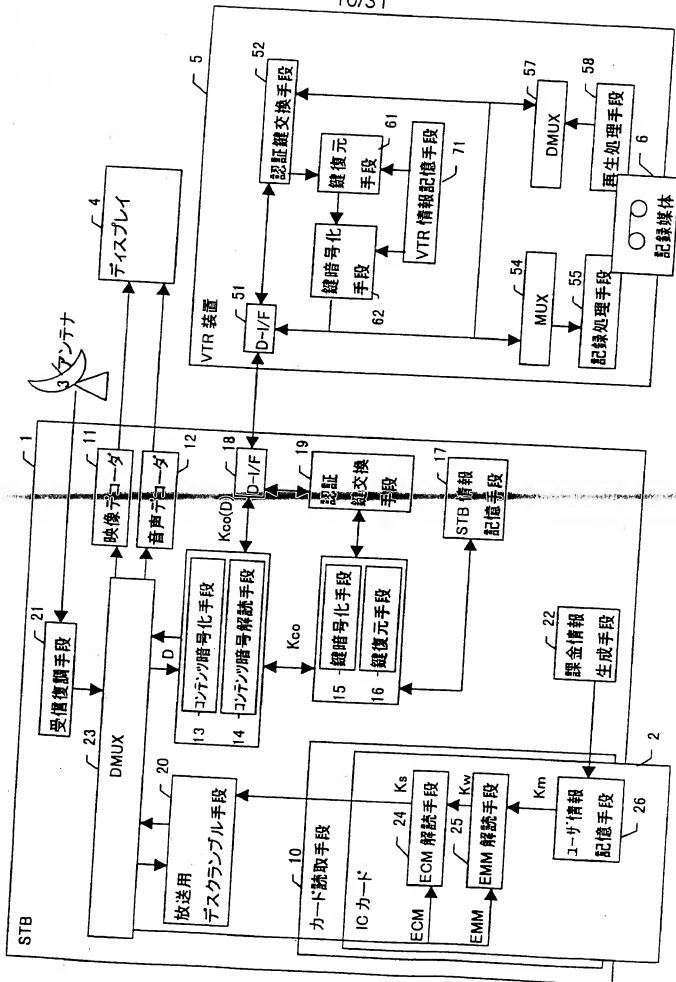
9/31

第9図

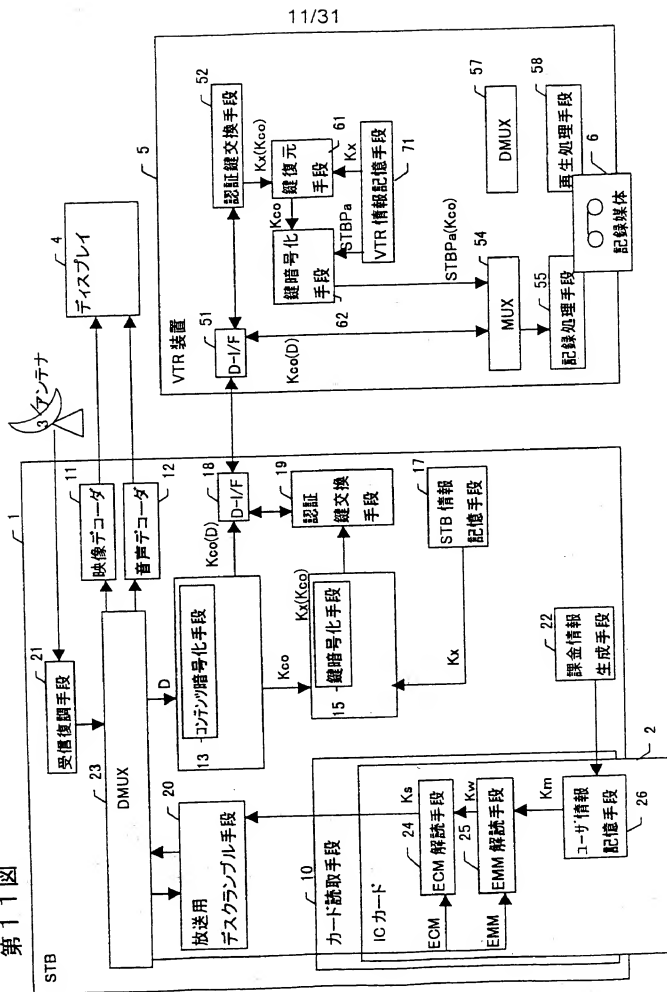


10/31

10 冊



第11図

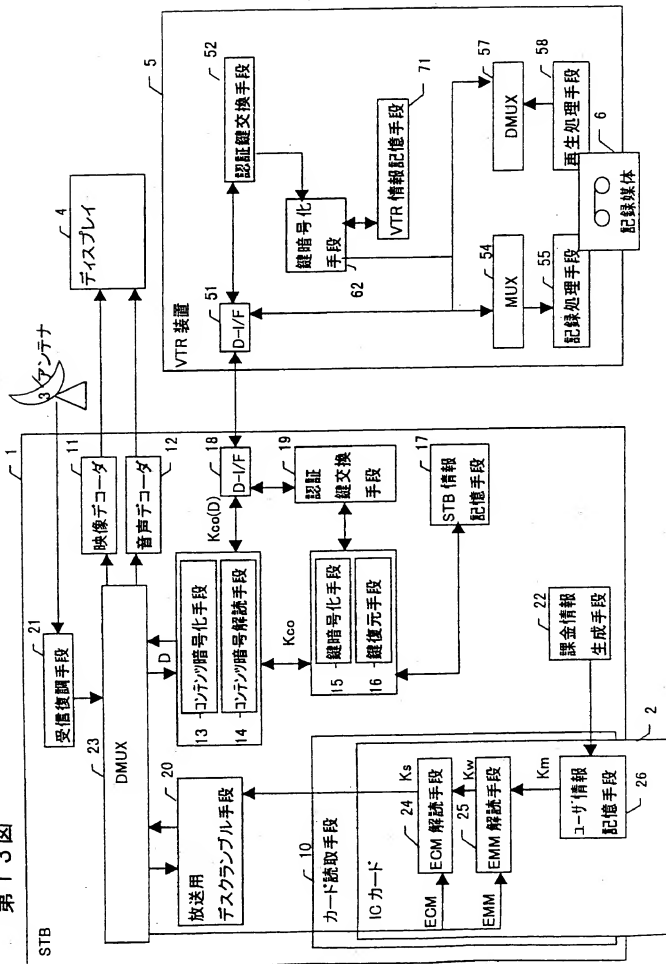






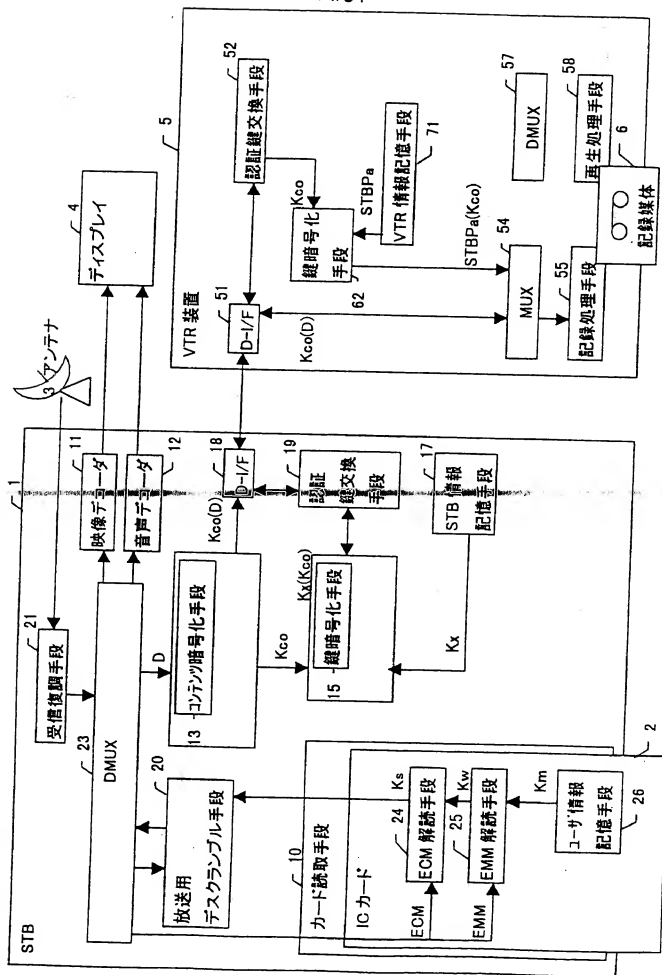
13/31

第13図



14/31

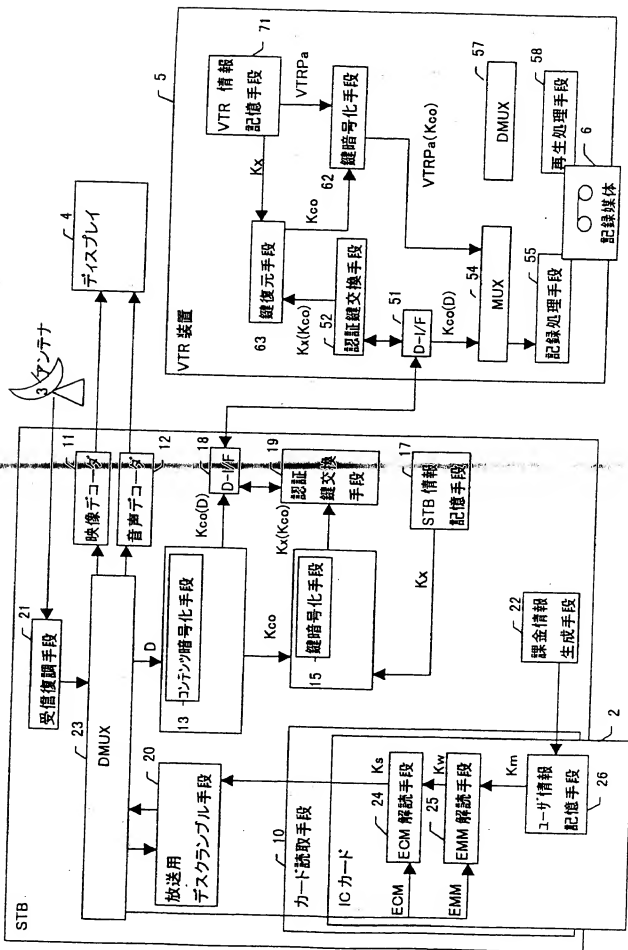
第14図





16/31

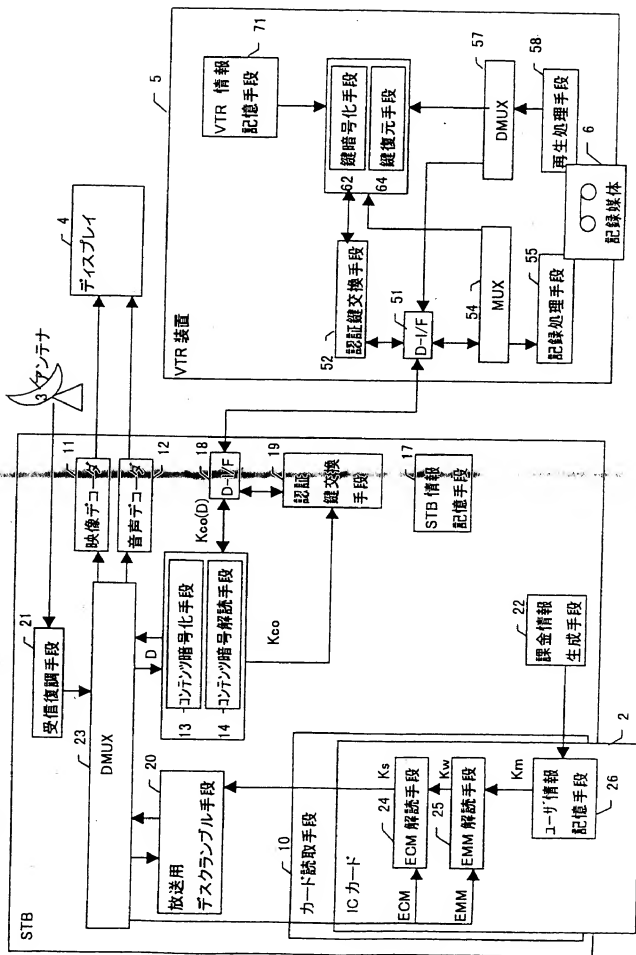
第16図





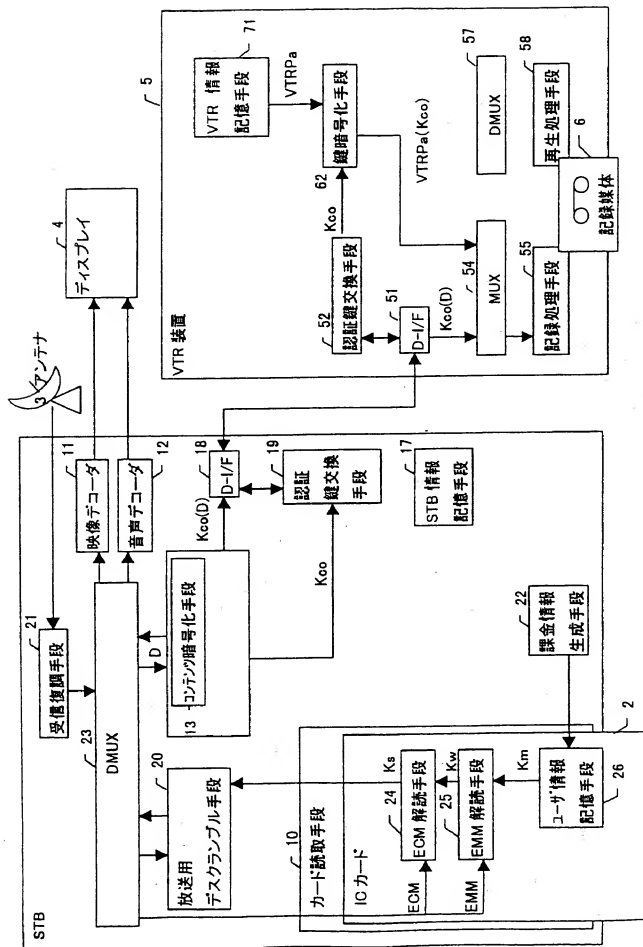
18/31

第18図



19/31

第19図

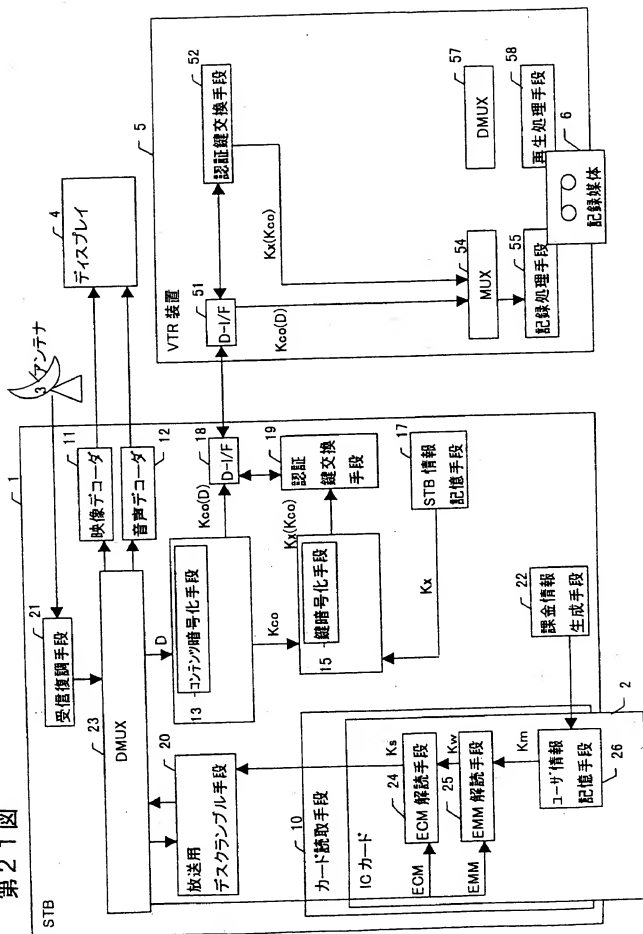






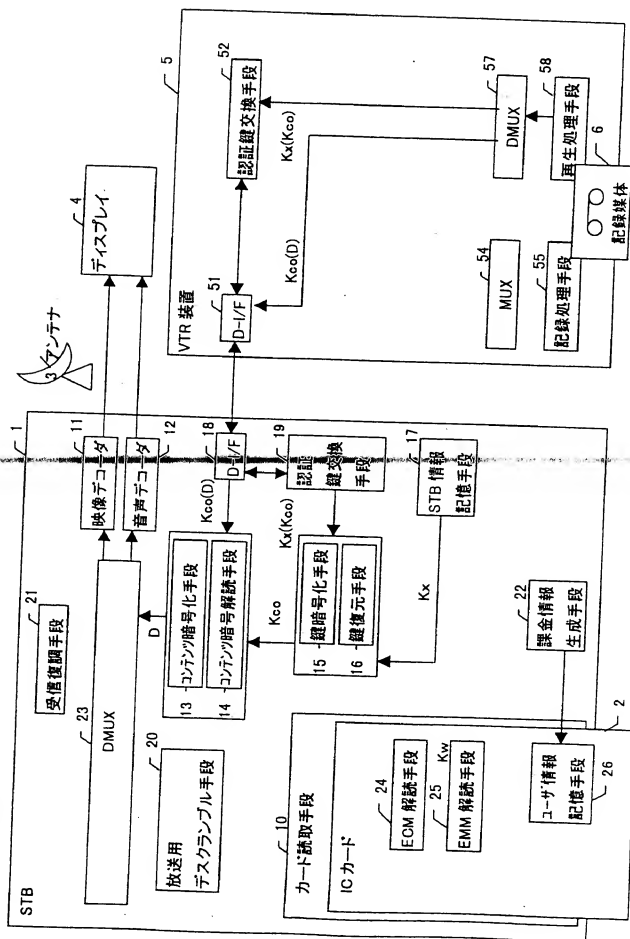
21/31

第21図



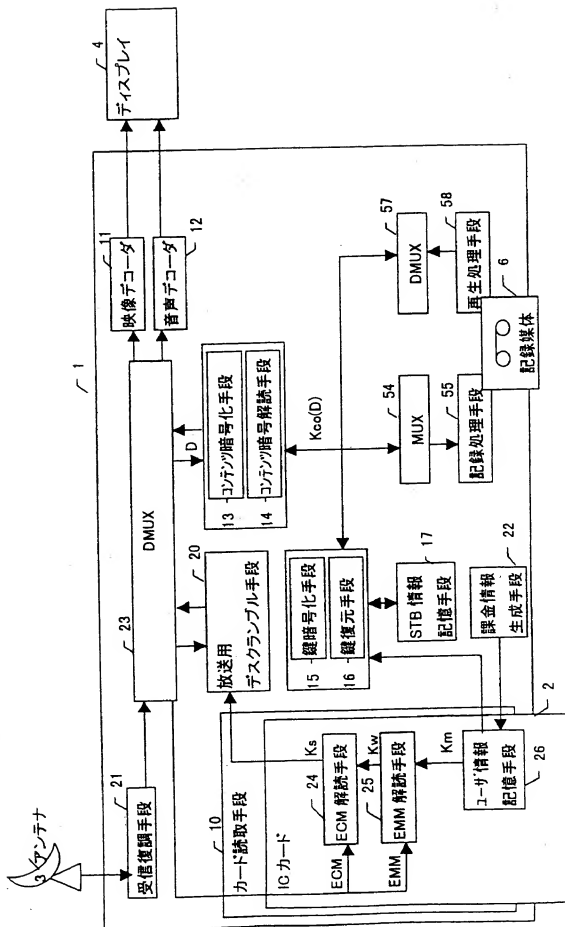
22/31

## 第22図

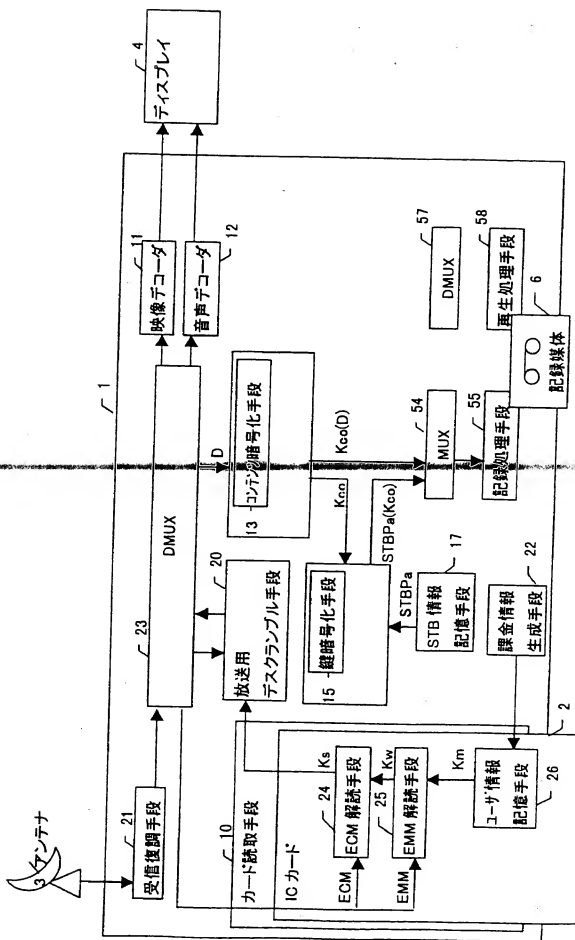


23/31

第23図

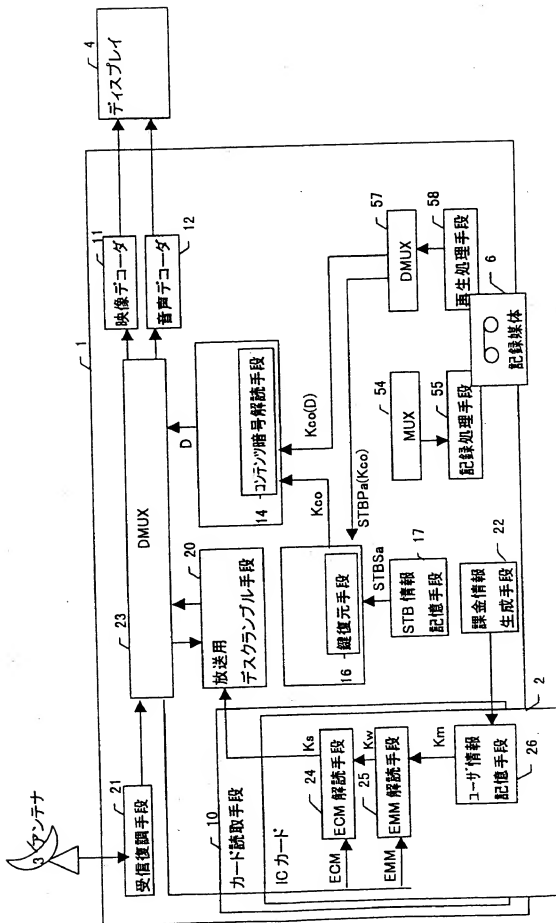


第24圖



25/31

第25図





27/31

## 第 27 図

暗号化鍵 Kx リスト

(a) 1 月 4 日現在

No.	暗号化鍵	鍵発生日
1	Kc4	1 月 4 日
2	Kc3	1 月 3 日
3	Kc2	1 月 2 日
4	Kc1	1 月 1 日
5		
6		
7		

(b) 1 月 9 日現在

No.	暗号化鍵	鍵発生日
1	Kc9	1 月 9 日
2	Kc8	1 月 8 日
3	Kc7	1 月 7 日
4	Kc6	1 月 6 日
5	Kc5	1 月 5 日
6	Kc4	1 月 4 日
7	Kc3	1 月 3 日







30/31

第30図

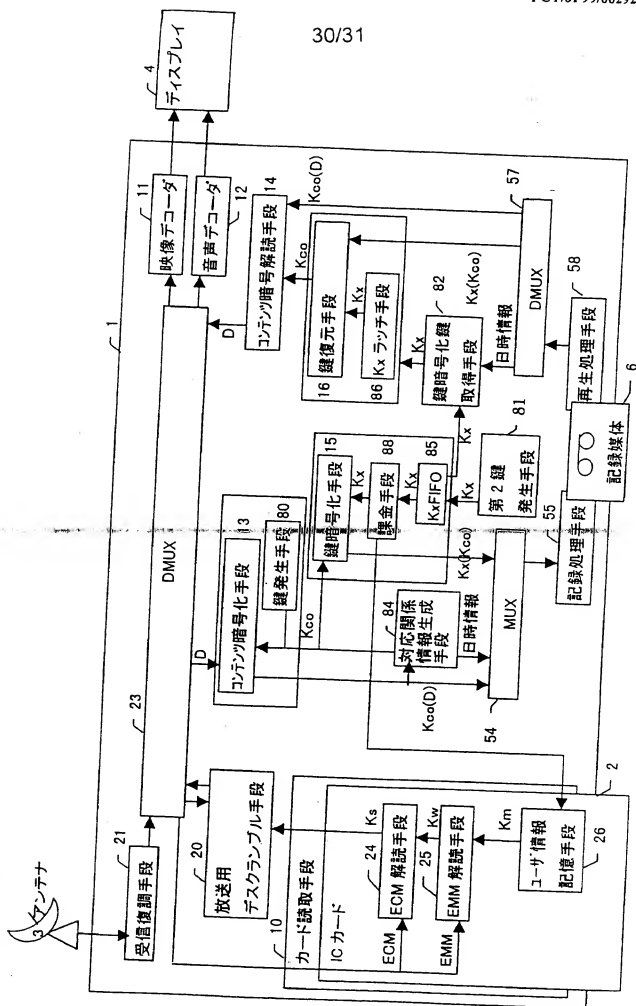
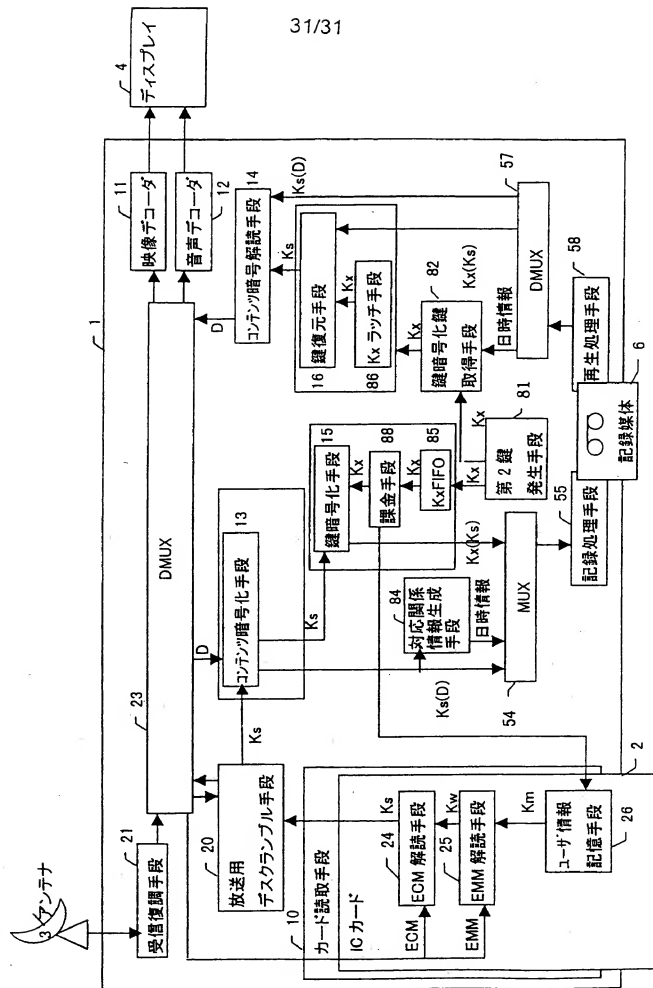


図 31 集



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/00292

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl.<sup>6</sup> G11B20/10, H04N5/91

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl.<sup>6</sup> G11B20/10, H04N5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999  
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	JP, 7-272399, A (Hitachi, Ltd.), 20 October, 1995 (20. 10. 95), Full text ; Figs. 1 to 18	1, 4, 6 2, 3, 5 7-66
X	Full text ; Figs. 1 to 18	
Y	Full text ; Figs. 1 to 18	
A	Full text ; Figs. 1 to 18 (Family: none)	
A	JP, 7-288798, A (Mitsubishi Electric Corp.), 31 October, 1995 (31. 10. 95), Full text ; Figs. 1 to 10 (Family: none)	11-14, 21
A	JP, 9-214929, A (Toshiba Corp.), 15 August, 1997 (15. 08. 97), Full text ; Figs. 1 to 6 (Family: none)	22-28
A	JP, 8-77706, A (Sony Corp.), 22 March, 1996 (22. 03. 96), Full text ; Figs. 1 to 7 (Family: none)	39-62

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

- \* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier document but published on or after the international filing date  
 "L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
19 April, 1999 (19. 04. 99)

Date of mailing of the international search report  
27 April, 1999 (27. 04. 99)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

## 国際調査報告

国際出願番号 PCT/J P99/00292

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>8</sup> G11B20/10, H04N5/91

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>8</sup> G11B20/10, H04N5/91

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
 日本国公開実用新案公報 1971-1999年  
 日本国登録実用新案公報 1994-1999年  
 日本国実用新案登録公報 1996-1999年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 7-272399, A (株式会社日立製作所) 20. 10月. 1995 (20. 10. 95)	1, 4, 6
Y	全文, 第1-18図	2, 3, 5
A	全文, 第1-18図 (ファミリーなし)	7-66
A	J P, 7-288798, A (三菱電機株式会社) 31. 10月. 1995 (31. 10. 95)	11-14, 21
A	全文, 第1-10図 (ファミリーなし) J P, 9-214929, A (株式会社東芝) 15. 8月. 1997 (15. 08. 97)	22-28
	全文, 第1-6図 (ファミリーなし)	

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリ

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって明である組合せによって進歩性がないと考えられるもの

「&amp;」同一パテントファミリー文献

国際調査を完了した日

19. 04. 99

国際調査報告の発送日

27.04.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

小松 正

5Q

7736

電話番号 03-3581-1101 内線 6922

様式PCT/ISA/210 (第2ページ) (1998年7月)

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 8-77706, A (ソニー株式会社) 22. 3月. 1996 (22. 03. 96) 全文, 第1-7図 (ファミリーなし)	39-62